2020-03

A secure and interoperable blockchain-based information sharing system for healthcare providers in developing countries

Kombe, Cleverence

NM-AIST

A SECURE AND INTEROPERABLE BLOCKCHAIN-BASED INFORMATION SHARING SYSTEM FOR HEALTHCARE PROVIDERS IN DEVELOPING COUNTRIES

Cleverence Kombe

A Dissertation Submitted in Partial Fulfilment of the Requirements for the Degree of Doctor of Philosophy in Information and Communication Sciences and Engineering of the Nelson Mandela African Institution of Science and Technology

Arusha, Tanzania

March, 2020

ABSTRACT

Systems in the health sector are very crucial for human life and they should be efficient, reliable and secure. Unfortunately, electronic health record (EHR) systems do not work effectively when managing multi-institutional medical records. The EHR, which is a digital system in which patient health information is systematically stored. The information stored includes medical history, laboratory test results, demographics, and billing information, poses problems to patients related to interoperability, privacy, and data integrity. Most solutions to these threats focus on a centralized architecture that faces a single point of failure and internal threats, such as unreliable system administrators.

The promising solution that many researchers are interested in is the use of blockchains. However, in developing countries, and particularly in sub-Saharan Africa, very little attention has been given to the issues of interoperability, privacy and data integrity for EHRs using blockchain technology. As such, this research has designed and developed self-sovereign identity management and secure information sharing system for health systems in developing countries, based on blockchain technology, which helps to solve the mentioned problems.

The study used a Design Science Research (DSR) methodology to develop solutions to the research problem through three sub studies. The first and the second sub studies conducted under problem awareness and suggestion phases of DSR, and third sub study conducted under development and evaluation phases of DSR. The first sub study deal with the assessment of three most common blockchain based healthcare systems (MedicalChain, Patientory, and MediLedger). The second sub study studies the problem of existing EHR systems in Tanzania regarding privacy issues in identity management and secure sharing of medical data from one healthcare facility to the other. The third sub study deal with the development of two systems, one for identity management using blockchain (self-sovereign identity), and one for secure sharing of medical data from one healthcare facility to another through blockchain technology.

The systems provide additional privacy protection tools to the existing infrastructures. They reduce development cost, transparency, data integrity, protection against single-point-of-failure vulnerabilities, and prevention of internal threats such as untrusted system administrators. The systems will make the existing and future health information systems trustable to healthcare service providers and the end-users of the healthcare systems. Also, will help the stakeholders in the healthcare sector to properly manage the healthcare systems.

DECLARATION

I, **CLEVERENCE KOMBE** do hereby declare to the Senate of Nelson Mandela African Institution of Science and Technology that this dissertation is my own original work and that it has neither been submitted nor being concurrently submitted for degree award in any other institution.

Cleverence Kombe

Name and signature of candidate Date

The above declaration is confirmed

Dr. Anael Sam

Name and signature of supervisor 1 Date

Dr. Mussa Ally Dida

Name and signature of supervisor 2 Date

Dr. Auvo Finne

Name and signature of supervisor 3 Date

COPYRIGHT

CERTIFICATION

The undersigned certify that they have read and found the dissertation acceptable by the Nelson Mandela African Institution of Science and Technology.

Dr. Anael Sam

Name and signature of supervisor 1 Date

Dr. Mussa Ally Dida

Name and signature of supervisor 2 Date

Dr. Auvo Finne

Name and signature of supervisor 3 Date

ACKNOWLEDGEMENT

I would like to thank God Almighty because without his graces and blessings this work would not have been possible. Also, I would like to express my heartfelt thanks to my family. Without their love and support over the years, none of these would have been possible. They have been there for me and I am thankful for everything they have helped me to achieve. I would like also to thank my supervisors, Dr. Anael Sam, Dr. Mussa Ally and Dr. Auvo Finne for their guidance without which I would not be where I am today. I would like to thank all friends specifically Mr. Bakari Sheghembe, Mr. Shadrack Daud, Mr. Emmanuel Nemes Shirima, and Mr. Venance Shija, for their friendship and support.

Also, I wish to express my sincere thanks to all my fellow students at NM-AIST specifically for their educational and friendship support. My special thanks also go to the course instructors at NM-AIST for their priceless assistance, extensive feedback and valuable suggestions regarding my studies. My heartfelt thanks to Dr. Goodiel Moshi, Dr. Majuto Manyilizu and Prof. Aloys Mvuma for their great effort in helping me achieve this dream.

Finally, it would certainly be remiss of not mentioning the Business School and Humanity (BuSH) course facilitators for their efforts to facilitate their courses during my first year at NM-AIST. I am also extending my deepest thanks NM-AIST Management, Finish Christian Medical Society (FCMS) through E-Health projects in Tanzania, Student's Organization (NMAIST-SO), the NM-AIST Librarians, the NM-AIST COCSE lab technicians and whole NM-AIST community for their constant co-operation and assistance with me during the course of my study.

DEDICATION

This dissertation is dedicated to my parents, Mr. Jerald Kombe and Mrs. Eunice Kombe. Thanks for making me be who I am today.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS AND SYMBOLS

AIDA	Agency for Integration, Diffusion and Archive of Medical Information
ALMC	Arusha Lutheran Medical Centre
API	Application Programming Interface
BTF	Byzantine Fault Tolerance
CA	Certificate Authority
CDO	Care Delivery Organization
CoCSE	School of Computation and Communication Science and Engineering
CPU	Central Processing Unit
CSSC	Christian Social Services Commission
Ctx	context
DDoS	Distributed denial of service
DHIS II	District Health Information Software II
DHT	Distributed Hash Table
DPoS	Delegated Proof of Stake
DSR	Design Science Research
EHR	Electronic Healthcare Records
EL	Electronic Ledger
EMR	Electronic Medical Record
Fabric CLI	Fabric Command Line Interface
GB	Gigabyte
GHz	Gigahertz
HIE	Health Information Exchanges
HL7	Health Level Seven
I/O	Input/ Output
ICT	Information Technology and Communication
IP	Internet Protocol
IPFS	Interplanetary File System
IT	Information Technology
JADE	Java Agent Development
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocols
Merkle DAG	Merkle Directed Acyclic Graph

MoHSW	Ministry of Health and Social Welfare
MSPs	Membership Service Providers
MTUHA	Mfumo wa Taarifa za Uendeshaji Huduma za Afya
NHIF	National Health Insurance Fund
NM-AIST	Nelson Mandela African Institution of Science and Technology
OpenEMR	Open Electronic Medical Record
OR – TAMISEMI	Ofisi ya Rais Tawala za Mikoa na Serikali za Mitaa
Org1	Organisation 1
Org2	Organization 2
Org3	Organization 3
PMEM	Physical Memory
PoS	Proof of Stake
PoW	Proof-of-Work
RAM	Random Access Memory
RDBMS	Relational Database Management System
SDK	Software Development Kit
SQL	Structured Query Language
TCRA	Tanzania Communications Regulatory Authority
TPC	Transactions Per CPU
TPDIO	Transactions Per Disk Input /Output
TPMS	Transactions Per Memory Second
TPND	Transactions Per Network Data
TPS	Transactions Per Second
TRA	Tanzania Revenue Authority
UML	Unified modelling language
VMEM	Virtual Memory

CHAPTER ONE

INTRODUCTION

1.1 Background of the problem

Electronic Healthcare Records (EHR) provide an easy way to share medical information between stakeholders such as consumers, healthcare providers, employers and payers, insurance companies and the government, and to assist patients through various care delivery organization (CDOs) such as hospitals, health centres, and dispensaries (Garets & Davis, 2005). On the other hand, Blockchain is an electronic registry of cryptographically hashed, authenticated, and controlled over a distributed network of computers using a group consensus protocol (Antonopoulos, 2015; Nakamoto, 2008). This adds additional confidence and privacy to the existing internet (Swan, 2015).

The healthcare systems are critical to human life. Systems in this sector must be efficient, reliable and secure. Unfortunately, the most of EHR does not work effectively when it comes to managing the multi-institution lifetime health records (Ekblaw *et al*., 2016). These systems have interoperability, privacy, and data integrity issues (Ozair *et al*., 2015). Globally, many countries, especially the west, are seeking solutions to these problems. Most solutions focus on centralized architecture, including solutions such as the Agency for Integration, Diffusion and Archive of Medical Information (AIDA) platform, Java Agent Development (JADE) technology, and Health Level Seven (HL7) standards (Cardoso *et al*., 2014; HL7, 2017; Miranda *et al*., 2013). Centralized architecture systems run the risk of a single point of failure and internal threats such as untrusted administrators (Laudon & Laudon, 2016).

1.2 Rationale of the study

The promise solution to interoperability, privacy, and data integrity problems which interests many researchers is the use of blockchain technology which focuses on distributed architecture (Goldwater, 2016; Krawiec *et al*., 2016; Samuel, 2016). Gropper's (2016) and Linn's (2014) works articulate that the use of blockchain technology offers an ability to protect patient data from different devices connected to the network. Furthermore, blockchain technology provides access privileges to patients on a type of data they want to share; also provides an entrance into interoperability. Estonia is the first country to create its national blockchain to protect patient information. Currently, health records of more than 1 million of Estonian citizens are protected by blockchain (Auffray *et al*., 2016; Brodersen *et al*., 2016; Lemieux, 2016). Therefore, this

study employed blockchain technology to solve mentioned problems without eliminating the legacy EHR systems.

1.3 Statement of the problem

In sub-Saharan Africa, several studies have been conducted to reveal the problems in interoperability, privacy and data integrity with the EHRs systems. In Tanzania, for example, Nehemiah (2014) and Kajirunga and Kalegele (2015) discovered the problem of interoperability and security issues including the privacy of patient information and data integrity for EHRs from different hospitals. On top of that, Mtebe and Nakaka (2018) revealed a lack of interoperability between Care2x and HarmoniMD in a healthcare facility. Similarly, Kamau *et al.* (2018) and William (2017) reported security issues regarding EHR systems in Kenya, Mauritius and South Africa, these issues include lack of privacy and integrity of patients' data and interoperability between healthcare facilities.

The proposed solutions to these problems are based on a centralized architecture. For instance, Ndume *et al.* (2013) focused on using Dynamic Link Library (DLL) for collecting e-health data to solve the problem of interoperability between different EHRs, but the system relies on centralized architecture whereby it may face single point of failure and/or inconsistency of data. This study failed to find literature evidence on the focus of using blockchain technology to solve the problem of privacy and integrity of patients' data and interoperability of healthcare systems in sub-Saharan Africa countries particularly in Tanzania by integrating existing EHRs with blockchain technology. Therefore, the study tries to bridge this gap by researching the way of solving mentioned problems without removing the legacy EHR systems using blockchain technology.

Blockchain technology is distributed architecture in nature with protection against centralized architecture's vulnerabilities. In healthcare, blockchain technology has been applied in the development of brand new EHRs systems and not applying it to the existing healthcare infrastructure to integrate different EHRs from different healthcare facilities in sub-Saharan Africa. As such, this research aimed to design interoperable and secure information sharing systems for healthcare systems for the existing EHRs infrastructures based on blockchain technology which will help in solving mentioned weaknesses while maintaining cost efficiency.

1.4 Objectives

1.4.1 Main objective

This study's target was to develop a secure and interoperable blockchain-based information sharing system for healthcare providers in developing countries' environment.

1.4.2 Specific objectives

In order to meet the main objective, the study aimed at fulfilling the following specific objectives:

(i) To investigate the capabilities of the currently available blockchain-based applications for healthcare information systems.
(ii) To analyse the requirements of applicable blockchain-based applications most appropriate for developing countries' environment.
(iii) To develop the blockchain based system for healthcare providers.
(iv) To evaluate the developed system.

1.5 Research questions

This study is intended to find answers to the following research questions:

(i) What are the capabilities of the currently available blockchain-based applications for healthcare information systems?
(ii) What are the blockchain-based requirements applicable for healthcare information system in developing countries environment?
(iii) What are the most effective design, coding and verification methods of a blockchain based system appropriate for healthcare providers?
(iv) Did the proposed system developed in a right way?

1.6 Significance of the study

This study leads to development of blockchain based systems that will add privacy protection tools to existing infrastructures, increase data integrity, protect against single-point-of-failure vulnerabilities, ensure secure sharing of medical information from one healthcare facility to another, and prevention of internal threats such as untrusted system administrators. In addition to that, the study helps the stakeholders in the healthcare sector to properly manage the

healthcare systems. Furthermore, this study contributes to knowledge whereby other researcher benefits its findings.

1.7 Delineation of the study

The study was confined to healthcare facilities (i.e. hospitals, health centres, and dispensaries) with fully installed EHRs in mainland Tanzania. The reason for choosing healthcare facilities with installed EHRs was because the study deals with improving the existing healthcare information systems and not developing a brand new EHR(s). Due to the sensitivity of the healthcare information systems and limited financial resources, this study developed and tested the prototypes in a virtualized environment. The prototypes can be implemented by other researchers, developers and stakeholders in a real world environment.

CHAPTER TWO

LITERATURE REVIEW

2.1 Overview

This chapter provides a comprehensive description of healthcare systems and blockchain technology. Interoperability, data integrity and privacy in health systems are explained. Blockchain technologies such as smart contracts and consensus protocols are also introduced.

2.2 Healthcare systems and healthcare stakeholders

Healthcare information system is a digital system in which patient health information is systematically stored. The information stored includes medical history, laboratory test results, demographics, and billing information (Garets & Davis, 2005). The health system is made up of all formal and informal public and private institutions, organizations and resources to promote, restore or maintain people's health (White, 2015). A health system not only includes facilities used to provide health services available in healthcare facilities, but also involves stakeholders such as a grandmother, who cares for a sick child at home, a private health professional, rehabilitation programs, campaigns of vector control, health insurance companies and researchers just to name a few (World Health Organization, 2007, 2017).

Properly configured health information systems help decision-makers to accurately identify the progress, needs, and problems facing the field. In addition, they allow them to make evidence-based policy and problem decisions. In developing countries, specifically in sub-Saharan Africa, health information systems are poorly configured. Main reasons identified as lack of health and IT professionals; rapid population growth that exceeds available health professionals; high cost of telecommunications; civil unrest and unstable power just to name a few (Ahlan & Isma, 2014; Fielding *et al.*, 2016; Miranda *et al*., 2013).

Some countries like Ghana, Uganda, Zambia, and Tanzania have recently introduced technological involvement in the health sector. Information and Communication Technology (ICT) has been used to reduce errors through automation of data collection, validation, and analysis. More industry engagement is still needed to ensure health data security and improve interoperability between different stakeholder systems. Therefore, existing healthcare information systems failed to solve problems related to interoperability, privacy of patients' private information and data integrity (Ahlan & Isma, 2014; Fielding *et al.*, 2016; Miranda *et al*., 2013; Mutale *et al.*, 2013; Nguyen *et al.*, 2014).

2.3 Interoperability, data integrity, and privacy in healthcare systems

In healthcare, suitable interoperable EHR systems provide greater efficiency, lower operating costs and save time in service delivery. Interoperability is the process of communication, data exchange, and the use of data exchange between different information technology systems and software applications. The data exchange scheme and standards allow data to be shared among different stakeholders, such as a clinician, laboratory, hospital, pharmacy, and patient, regardless of application or application vendor. In health systems, interoperability is the ability of health information systems to work together, both inside and outside the organization (Cardoso *et al.*, 2014; Miranda *et al.*, 2013).

Integrity, on the other hand, ensures that data stored or exchanged between EHRs is accurate and unchanged. Data loss or destruction that occurs during data transfer raises concerns about database accuracy. EHRs must ensure patient safety by minimizing health errors, reducing health disparities and improving public health. In addition, the theft of medical identity leads to inaccurate information being entered in the victim's record. The victim's insurance company will be charged for medical services that are not provided to the actual policyholder, and the future treatment of the patient will be guided by a manufacturing facility that is not immediately identified by either the patient or the care provider (Nelson & Staggers, 2016; Rahman, 2014).

Additionally, lack of trust in Electronic Health Records (EHRs) and Health Information Exchanges (HIEs), i.e. patients feeling that the confidentiality and accuracy of their electronic health information are in jeopardy, they may not want to disclose health information to the system. Revealing the patients' health information could have serious consequences. Therefore, it's very important for EHRs to ensure the privacy and security of health information (Soceanu *et al.*, 2015; William, 2017).

On top of that, when breaches of health information occur, they can have damaging consequences for an organization, including reputational and financial harm or harm to the patients. Poor privacy and security practices increase the vulnerability of patient information in EHRs, increasing the risk of successful cyber-attack. Therefore, since existing healthcare information systems failed to solve problems related to interoperability, privacy of patients' private information and data integrity, integrating blockchain technology seems to be an appropriate solution (Soceanu *et al.*, 2015; William, 2017).

2.4 Blockchain technology

Blockchain is an electronic registry of cryptographically hashed, authenticated, and controlled over a distributed network of computers using a group consensus protocol (Fig. 1). Consequently, it adds confidence and confidentiality to the existing internet. The blockchain network is inexpensive and efficient due to its ability to remove duplication and reduces the need for intermediaries, hence result in low operating cost comparing to non-blockchain network. It is also less susceptible to attacks because it uses proven models to verify the information, therefore, transactions are secure, authenticated, and verifiable (Antonopoulos, 2015; Nakamoto, 2008; Swan, 2015).

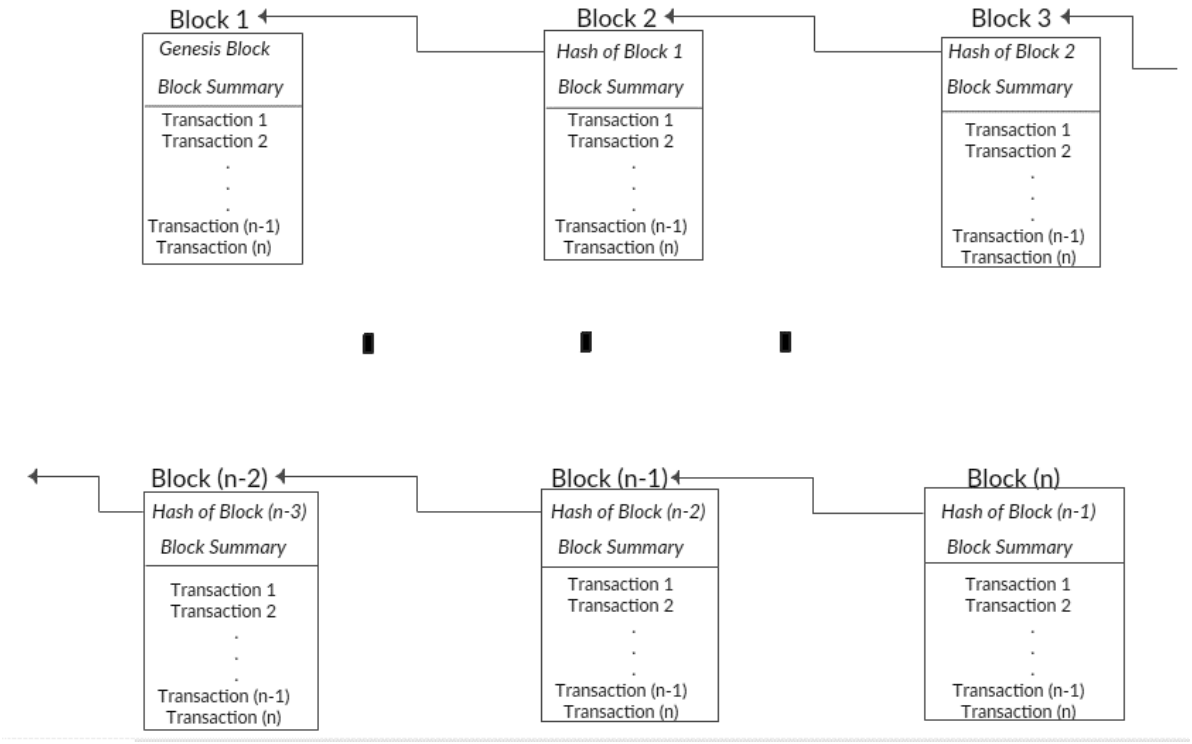

Figure 1: The main concept of blockchain

Blockchain security features protect internet-connected systems from hacking, fraud, and cybercrime. If the blockchain network is permissioned, it allows you to create a network only for members with proof that the participants are who they claim to be and that the exchange of transactions exactly matches those presented. In addition, the blockchain enhances privacy by using credentials and permissions, users can specify which details of the transaction they want other participants to be able to view. Permissions can be extended for special users, such as auditors, who may need access to more detailed transaction information, etc (Laurence, 2017; Tapscott & Tapscott, 2016).

Blockchains are classified into permissionless or permissioned. Systems without permission are open networks where any peer can transact and participate in a consensus activity to move the system forward. They are accessible in public, so the number of peers is projected to be huge and these peers are anonymous and unreliable because any peer can be connected to the system (i.e. bitcoin and ethereum). The permissioned blockchains, however, are closed, through which transactions can be made by any peer, but the activity to move the network forward is constrained to the fixed number of peers that are executed through consortium nodes. Frameworks such as Multichain and hyperledger fabric are meant at consortia where involvement is limited. Some studies propose that for confidentiality, safety purposes, and privacy hyperledger blockchains are safer than ethereum (Androulaki *et al.*, 2018; English *et al.*, 2018; Reyna *et al.*, 2018; Peters & Panayi, 2016; Sousa *et al.*, 2017).

Hyperledger fabric is a blockchain infrastructure for running distributed applications. Only registered participants are permitted to read/write in the hyperledger fabric ledger. This configuration makes it easier to control transactions in the ledger and is usually faster than public blockchain where participants are not registered in the ledger. Peer nodes execute chain codes (smart contracts), access ledger data, approve transactions, and interface with applications. Orderer nodes provide blockchain consistency and deliver trusted transactions to network peers, and Membership Service Providers (MSPs), typically implemented as a certificate authority, handling the X.509 certificates used to authenticate the nodes. Hyperledger fabric implements channels, whereby the data of a channel is only visible to members of that channel, but not to other peers in the network (Benhamouda *et al.*, 2019; Yamashita *et al.*, 2019).

According to Agarwal (2019) and Shu *et al.* (2019) hyperledger fabric runs through the following phases; simulation, ordering, validation, and commit. In the simulation phase, an application node sends a transaction proposal to endorsement nodes. Because organizations do not fully trust each other, at least one node of each participating organization simulates the transaction proposal. The endorsers simulate in parallel the transaction proposal against a local copy of the current status. Each endorser creates reading and writing set during the simulation to capture the effects. After the simulation, each endorser sends its read and write the record back to the application node. Then the application node forwards this transaction to the order service.

During the order phase, the trusted ordering service receives the transactions from the application node. Among all received transactions, the global order is created and packaged

into blocks with a certain number of transactions. By default, the transactions are essentially arranged as they come to the service, without the transaction semantics being checked in any way. The ordering service then distributes each formed block to all peers of the system network. Note that the system does not guarantee that all peers receive one block at a time. However, it is guaranteed that all peers receive the same blocks in the same order. The system does not ensure that all connected nodes receive one block at a time. But, in the end, all connected nodes will have the same blocks in the same order (Agarwal, 2019).

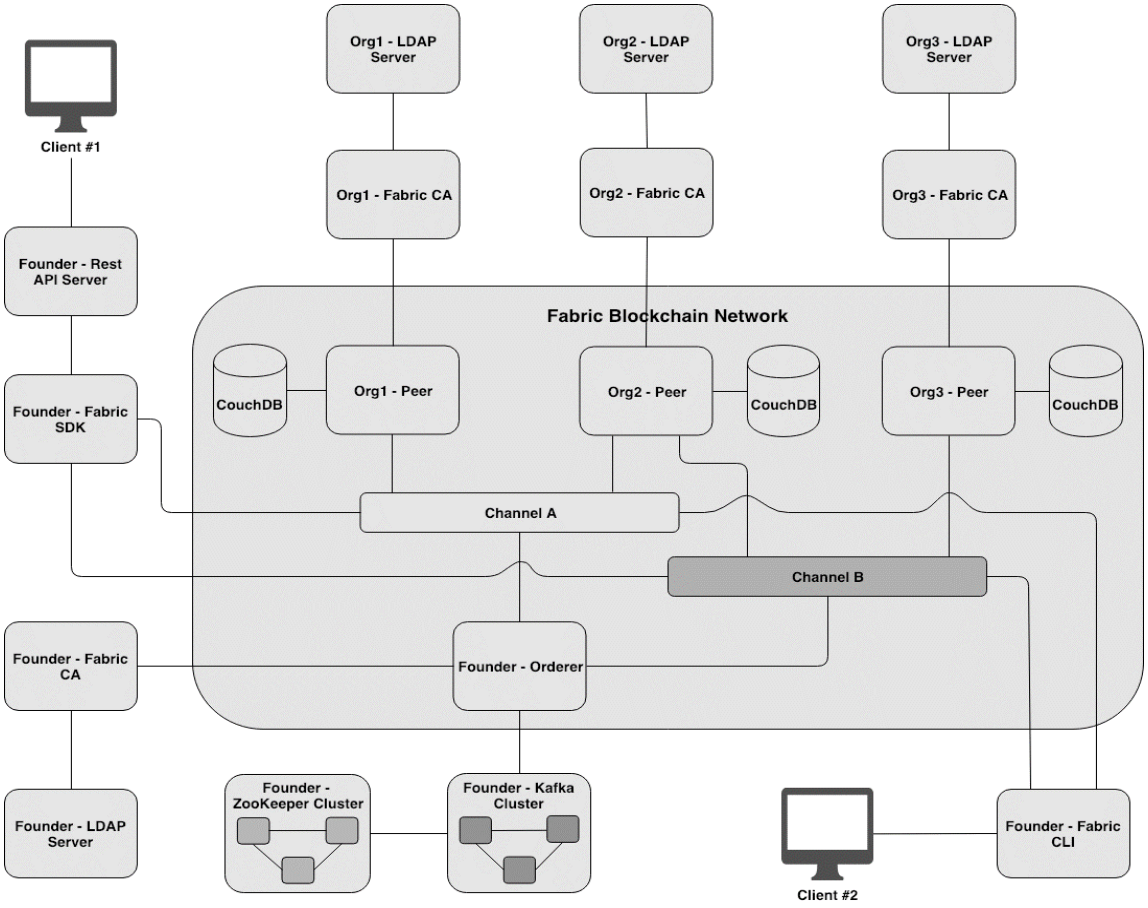

Figure 2: The general architecture of hyperledger fabric (Thummavet, 2019)

In the validation phase, the validation phase begins as soon as a block arrives at a peer. In any transaction within the block, validation has the following checks; First, fabric checks that the transaction complies with the endorsement policy and that all the signatures it contains match the read and write set. If not, this means that either an endorser or the client has manipulated the transaction in some way. In this case, the systems identify the transaction as invalid. Second, if a transaction passes the first test, fabric checks for serialization conflicts. Since the simulation of transactions runs parallel before their order, the effects of the simulation can be

in conflict with the specified order. Therefore, fabric also marks transactions that conflict with previous transactions as invalid (Agarwal, 2019; Shu *et al.*, 2019; Thummavet, 2019).

In the commit phase, each peer attaches the block containing both valid and invalid transactions to its local ledger. In addition, each peer applies all changes made by the valid transactions to its current status (Benhamouda *et al.*, 2019; Yamashita *et al.*, 2019). Figure 2 shows the architecture of hyperledger fabric.

2.4.1 Blockchain consensus protocols

Blockchain network performance is determined by the applied consensus protocol, a mechanism which allow the computers connected in blockchain to reach a common agreement on the state of transaction in the ledger. The consensus protocol plays an important role in upholding the efficiency and security of the blockchain. Consensus protocols must be robust against damaged messages, host failures, network breakdowns, message delays, and messages that fail. They must also handle selfish and intentionally malicious peers. The consensus in a blockchain system assures that all peers in the system approve the consistent global blockchain status (Milutinovic *et al*., 2016; Zheng *et al.*, 2016; Baliga, 2017; Laurence, 2017).

Table 1: Blockchain Consensus Protocols

Algorithm	***Hash Power***	***Number of Nodes***	***Identification of New Nodes***	***Transaction Verification Speed***
Proof of Work	Yes	Large	Public	Slow
Proof of Stake	Yes	Large	Public	Slow
Delegated Proof of Stake	Yes	Low	Private	Fast
Proof of Elapsed Time	Yes	Low	Private	Fast
Deposit-based consensus	Yes	Large	Public	Fast
Proof of Importance	Yes	Low	Private	Fast
Byzantine Fault Tolerance	No	Low	Private	Fast
Federated Byzantine Agreement	No	Low	Private	Fast
Proof of Work and Proof of Stake Hybrid	Yes	Large	Public	Slow
Proof of DDoS	Yes	Large	Public	Slow

Permissionless blockchain consensus protocols like Proof of Stake (PoS), Delegated Proof of Stake (DPoS) and Proof of Work (PoW) allow perpetual participation despite having problems in achieving low latency, immediate transaction end-to-end, good scalability, and high throughput. Permissioned frameworks, however, contains semi-trusted nodes, through which acknowledged participants take part in a consortium. The number of participants is low, which

is why it is easy to use alternative consensus algorithms than in a permissionless blockchain (Baliga, 2017; Mingxiao *et al*., 2017).

Consensus algorithms such as Byzantine Fault Tolerance, SIEVE, and Cross-Fault Tolerance are fast, consume little computational power, but cannot have indefinite participation (Table 1). To overcome these limitations, various protocols have been recommended in the literature, each algorithm making the necessary assumptions regarding safety of the messages being exchanged, synchronicity, message transfers, errors, malicious nodes, and performance (Eyal *et al.*, 2016; Hsieh *et al*., 2017; Sikorski *et al.*, 2017).

2.4.2 Smart contracts

Smart contracts are computer programmable codes deployed in a distributed blockchain architecture. Many healthcare professionals see blockchain and smart contracts as a safe way to share and access EHR. Smart contracts include signatures from multiple patient provider, so only authorized users or devices can access or attach the document. Smart contracts are created to facilitate, verify, or enforce the prenegotiated terms between two or more parties. The blockchain protocol takes the place of enforcement of contracts. Smart contracts, in effect, allow two or more parties to work together without trust or the need to have authoritative judgment or settlement if things go wrong (Xiong & Xiong, 2019; Xu *et al.*, 2017).

Hyperledger fabric uses container technology to hold smart contracts known as "chaincodes" that make up the logic of the system application. The "chaincode" is executed in computer languages like JavaScript, Java, Python and GO which is called by a transaction proposal. A smart contract is computed in the blockchain by a contract creation transaction. Once the contract creation transaction is included in the blockchain, the smart contract receives a contract address. Each smart contract consists a blockchain address that can be saved (Mohanta *et al.*, 2018; Thomas *et al.*, 2019).

2.5 Blockchain technology in healthcare

Healthcare systems require more efficiency and secured system for clinical records management, pre-authorization of payments, settlement of insurance claims and the execution and keeping of complex transactions. Blockchain delivers answers to these problems. Electronic patient records are presently stored in data centres, in which access is restricted to networks of hospitals and healthcare providers. Centralizing such data makes them susceptible to security breaches and can be costly to keep. To avoid this, blockchain keeps the complete clinical history of every patient with several control granularities for patients, physicians,

regulatory agencies, hospitals, insurers, etc., and provides a secure mechanism for recording and maintaining a complete clinical history for every patient. This guarantees tamper-proof storage of clinical history. Shorten processing time for insurance dues and increase the effectiveness in offering insurance services; and comprehensive patient history for use by doctors for accurate medicine prescriptions (Gropper, 2016; Gupta, 2017; Samuel, 2016).

CHAPTER THREE

MATERIALS AND METHODS

3.1 Overview

This chapter presents the methodology used in this study. The study used Design Science Research (DSR) to develop solutions to the research problem. Vaishnavi and Kuechler (2015) and Venable *et al.* (2017) explained that DSR is a good methodology for Information Technology (IT), Computer Science (CS), Information System (IT) and Software Engineering (SE) fields since research studies in these fields have to be conducted differently from Social Science or Life Science fields because of their nature of solving problems of other fields most of the time. Vaishnavi and Kuechler (2015) identified five phases for conducting research study through DSR: a) awareness of the problem; b) suggestion; c) development; d) evaluation/validation; e) and conclusion. These DSR phases were used in this study. Figure 3 illustrates the methodology used in this study.

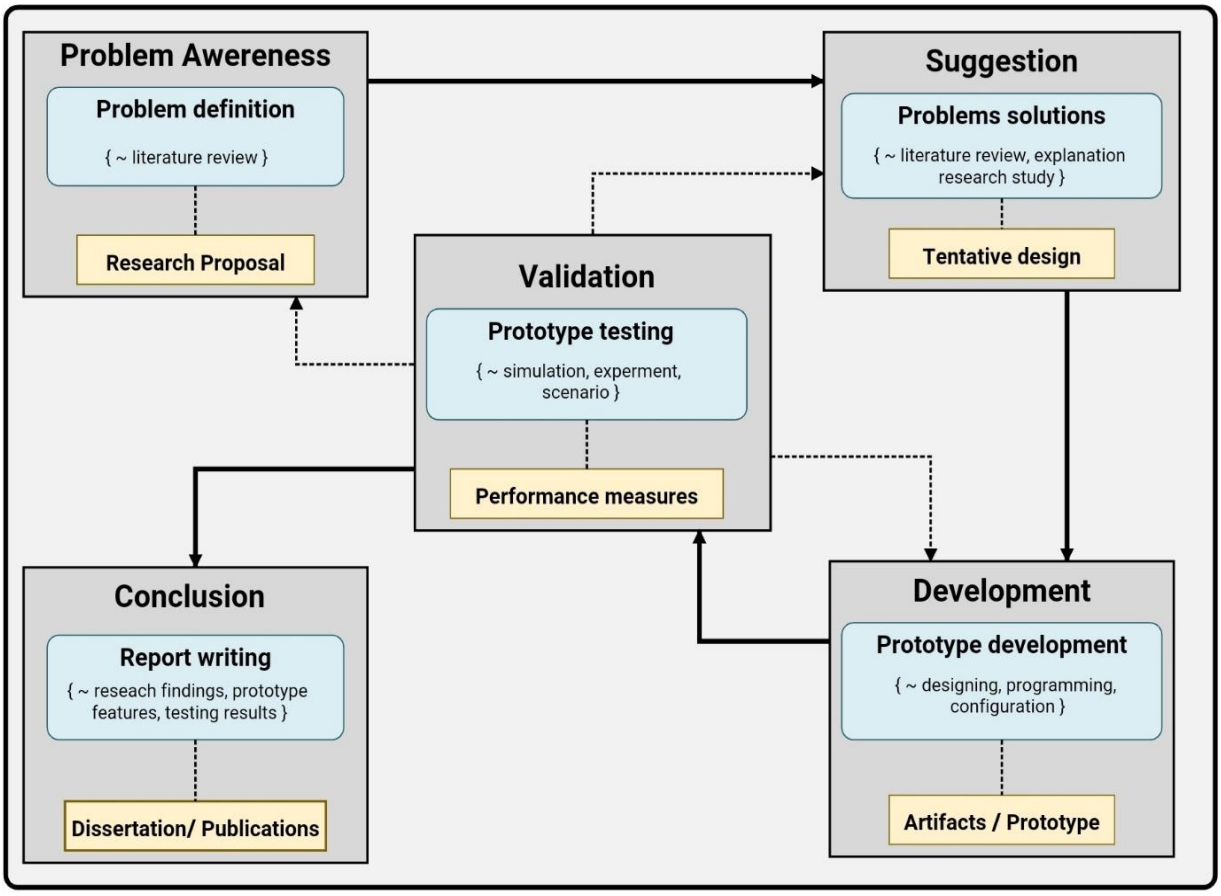

Figure 3: Design science research (DSR) methodology

3.2 Problem awareness

In the awareness phase, research issues were identified through literature research, interviews with health professionals, brainstorming with colleagues from the Nelson Mandela African Institution for Science and Technology (NM-AIST), discussion with supervisors and concept note presentation at the School of Computation and Communication Science and Engineering (CoCSE). These steps were taken in the problem awareness phase to ensure that the research problem was not defined and resolved elsewhere, and to ensure the contribution of problem-solving in the healthcare and research communities (Dresch *et al.*, 2015). The research proposal report and the oral presentation were carried out in the NM-AIST for evaluation.

3.3 Suggestion

The suggestion phase served to propose preliminary solutions to the research study through literature research and explanation research. Explanatory studies have used qualitative and quantitative methods to collect and analyse research data to identify possible proposals and to provide a preliminary design for the artefacts. According to Vaishnavi and Kuechler (2015), an explanatory research study may be applied in suggestion phase of DSR through quantitative and/or qualitative data collection and analysis techniques to explain why a certain phenomenon occurs. Various methods have been used to conduct an explanation research study. Aspects covered in the following subsections include the research design, study setting, data gathering procedures, and how data was collected and analysed. Moreover, ethical issues, as well as the reliability and validity of the collected data, are dealt with in the subsections.

3.3.1 Research design

Research design provides the basis for data collection and analysis (Bryman, 2012). It contains a description of what the researcher will do from writing the research question and their practical application to the final analysis of the data (Davis, 1989). The research design of this explanatory study is basically a case study, in which data were collected through qualitative interviews, direct observation, participant observation, documentary review, and an experiment that led to the collection of valid and reliable data.

3.3.2 The study setting

The study was conducted in public and private healthcare facilities in Tanzania. The choice of medical facilities was made specifically to include hospitals, health centres and dispensaries. Mainland Tanzania consists of 7167 medical institutions, of which 72.3% belong to the government, and the remaining 29.7% belong to private companies and organizations (Table

2) (CSSC, 2017). This study involved 710 medical facilities from mainland Tanzania, a proportionate stratified random sampling technique was applied with a sampling fraction of 1 in 10 to ensure each subgroup is represented in the study (Table 3).

3.3.3 Research approach

This explanatory study used quantitative and qualitative approaches. Bamberger (2000) states that mixing approaches increase the validity of research results. He reported that scientific research projects based on the objectivity of quantitative approaches are complemented by the quality of things like what, when, how, where of social issues; The essence of things - meaning, concept, definitions, properties, metaphors, symbols and descriptions of things that are all qualitative in nature.

Table 2: Distribution of healthcare facilities in Tanzania

	Ownership				
Category of Health Facility	Government	Parastatal	Faith-based	Private	**Total**
Hospitals	98 (39.7%)	8 (3.2%)	105 (42.5%)	36 (14.6%)	**247**
Health Centres	535 (74.9%)	10 (1.4%)	134 (18.8%)	35 (4.9%)	**714**
Dispensaries	4554 (73.4%)	168 (2.7%)	697 (11.2%)	787 (12.7%)	**6206**
Total	***5187 (72.3%)***	***186 (2.6%)***	***936 (13.1%)***	***858 (12.0%)***	***7167***

3.3.4 Target population and sampling procedures

This explanatory research used non-probabilistic sampling techniques involving different groups of health professionals. The respondents selected were heads of hospitals/healthcare facilities, ICT experts, government officials, physicians, nurses, lab technicians, pharmacists, accountants, and receptionists. The study also included directors and ICT experts from Ministry of the country - President's Office Regional Administration and Local Government (Wizara ya nchi - Ofisi ya Rais Tawala za Mikoa na Serikali za Mitaa (OR-TAMISEMI)) and the Commission for Christian Social Services (CSSC).

(i) Sample size

It is difficult to predetermine the sample size for qualitative studies because they are based on the nature and scope of the research subject, the resources available and the study design. Therefore, in qualitative research, the sample size is usually determined when data saturation is reached (Mason, 2010; O'reilly & Parker, 2013). Some studies suggest up to 10

homogeneous sample sizes for case study research (Creswell, 2015; Yin, 2015). Given this fact and the limited time involved in this study, four to six respondents were interviewed per expert group, resulting in a minimum of 50 respondents depending on the degree of overlap of expertise.

Table 3: Distribution of sample medical facilities involved in the study

	Ownership				
Category of Health Facility	Government	Parastatal	Faith-based	Private	**Total**
Hospitals	9	1	10	3	**23**
Health Centres	53	1	13	3	**70**
Dispensaries	454	16	69	78	**618**
Total (Sample)	***516***	***18***	***92***	***84***	***710***

(ii) Sampling method

Haq and Shabbir (2014) define samples as the selection of a suitable sample representative of the population from which it was taken to determine the parameters or characteristics of the entire population. The participants were purposively selected one after the other with an interdisciplinary approach to optimize variations and capture different views and experiences (Palinkas *et al*., 2015; Ritchie *et al*., 2013). Selected experts for purposive sampling included heads of hospitals/healthcare facilities, ICT experts, government officials, doctors, nurses, laboratory technicians, pharmacists, accountants, and receptionists. The researchers ensured that selected experts met two criteria; first, they cover the topic well and represent it. Second, diversity is included in each group of experts so that the impact of research issues can be monitored.

Researchers also used opportunistic sampling and convenience sampling due to unplanned opportunities in fieldwork. The researchers interviewed directors and ICT experts from Ministry of the country - President's Office Regional Administration and Local Government (Wizara ya nchi Ofisi ya Rais Tawala za Mikoa na Serikali za Mitaa (OR – TAMISEMI)) and Christian Social Services Commission (CSSC) because they manage the installation and maintenance of all healthcare information systems for government and faith-based healthcare facilities. Therefore, the researchers interviewed 50 respondents through purposive, opportunistic, and convenience sampling, including respondents from 710 health care institutions involved in the study.

The researcher applied proportionate stratified random sampling to select 710 medical facilities from 7167 medical facilities with a sampling fraction of 1 in 10 (Table 3). This sampling technique was selected to ensure each subgroup is represented in the study (Bryman, 2012). Other data collection methods, i.e. direct observation, participant observation, and documentary analysis were used to collect the required data from 710 healthcare facilities. Moreover, a letter of invitation with an information document was sent to the respondent or institution addressed. The letter of invitation emphasized that respondents, despite their backgrounds, attitudes to different issues faced by health systems, are eligible to participate. This was done to minimize participant bias, due to the oversampling of respondents.

3.3.5 Data collection methods and instruments

In order to gain a clear understanding of what is happening in the chosen field, data collection methods have been developed to help researchers to collect the data needed to answer the research questions and to link the data collected to the research proposals. Yin (2015) identifies six sources of evidence in case studies; these are documentary reviews, archive records, interviews, direct observation, participant observation, and questionnaires.

In this explanatory study, the researcher used qualitative interviews, documentation reviews, direct observations, participant observations, and experiments to increase information validity and reliability. Further, various data collection methods have been developed to help researchers collect data needed to answer the research questions and to link the collected data to the research proposal.

(i) The qualitative interviews

This study recognized the value of understanding health systems issues from different angles, such as perceptions and experiences of key stakeholders, to help decision-makers resolve EHR issues. Therefore, the researchers conducted qualitative interviews with stakeholders such as health facility leaders, ICT experts, government officials, physicians, nurses, laboratory technicians, pharmacists, accountants, and receptionists. The qualitative interview used in the study because it focuses on answering the research questions directly and giving researchers access to a wider variety of expertise and conditions (Bryman, 2016).

(ii) Direct observation and participant observation

Rubin and Babbie (2014) find that direct observation helps the researcher to see, observe physically and directly from a real concrete situation, which increases validity and reliability.

Direct observation and observation of participants was used in assessing the various functions of the system and the activities of experts.

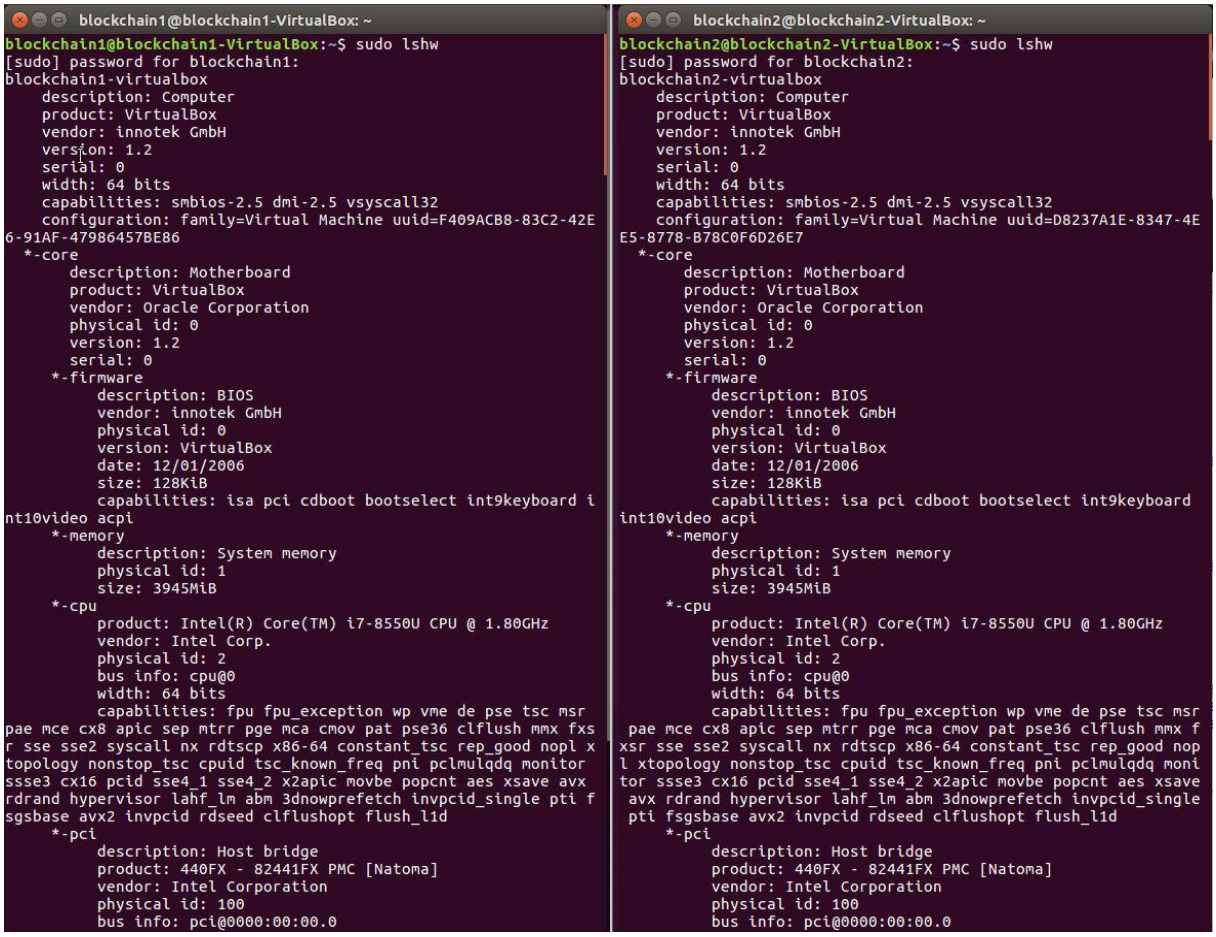

Figure 4: Configuration of operating system environment

(iii) Documentary review

The researchers used the analysis of documents from publicly available documents (mission statements, annual reports, guides, and strategic plans), personal documents (service journals, blogs, event reports, and newspapers) and physical evidence (leaflets, posters, reference works and training materials). Document analysis is an effective and efficient way to collect data because documents are clearer, more accessible, more reliable, less expensive, and more cost-effective than other methods (Bowen, 2009; O'Leary, 2004).

(iv) Experiment

The performance experiments executed in blockchain frameworks i.e. parity, ethereum, and hyperledger fabric. Tests were conducted using 1000 smart contracts in machines with Intel Core i7-4790 3.60 GHz CPU and 8 GB RAM. The investigated blockchain-based health applications were designated due to popularity, their blockchain type, and their general

functionalities. These applications are MediLedger on the private parity framework, Patientory run on the public ethereum framework, and MedicalChain on the consortium hyperledger fabric framework (Kombe *et al.*, 2018).

3.3.6 Data analysis procedure

The data was entered into the NVivo11 software, which was used to manage and organize the data analysis process. The framework approach was used to design the analysis process using the following steps: incorporating and commenting transcripts, identifying a thematic framework, indexing, drawing, mapping, and interpretation (Gale *et al*., 2013; Ritchie *et al.*, 2013). The mapping step is used to recognize relationships and clusters around topics that help in understanding, communication, and interpretation. Additionally, themes were used to show the most important problems from the data in understanding the views and experiences regarding the problems facing EHR systems. COREQ checklist used to guide the conduct, analysis, and reporting of this research (Booth *et al.*, 2014). Additionally, OriginPro 9.0.0 software used to assist the researcher in analysing the data obtained in experiments.

3.4 Development

The development phase attempts to implement the artefact according to tentative design or suggested solutions from the suggestion phase (Dresch *et al.*, 2015; Hevner & Chatterjee, 2010; Vaishnavi & Kuechler, 2015). This study developed two systems that were suggested in suggestion phase. The first system was a self-sovereign identity system for the existing electronic healthcare system infrastructures, and the second system was a decentralized and interoperable health information sharing system for the existing electronic healthcare system infrastructures. Both proposed systems utilized the blockchain decentralized architecture.

For the first system, the hyperledger indy framework used in a virtualized environment to add self-sovereign identity to two open-source electronic health record systems (Care2x and OpenEMR) on a connected network. Several programming languages used in developing different methods for the proposed system (Python, Java, JSON, and C++). Unified modelling language used in designing different artefacts (UML diagrams) through flowdia diagram and creately UML development tools.

The second system developed in the hyperledger fabric framework. The system was developed and configured in a virtualized environment by which two ubuntu 16.04 operating systems (Fig. 4) with 4GB of RAM and secondary storage of 30GB each were installed in VirtualBox 6.0.12. Several development tools were installed to allow hyperledger fabric 1.4.3 to run

smoothly. The tools are; cURL 7.6.5, Docker 18.09. Docker-compose 1.24, node.js 18.16.0, npm 5.6.0, Python 3. The smart contract for this system developed in JavaScript. Visual Studio Code version 1.36.0 used to assist a researcher in writing and editing code for different programming languages.

3.5 Evaluation

The evaluation phase which also known as the validation phase in some literature is used to determine how well the developed prototype work (Hevner & Chatterjee, 2010; Hevner, 2007). Methods similar to theory testing (i.e. experiments, simulation, or scenario) are used in the validation process (Dresch *et al.*, 2015; Vaishnavi & Kuechler, 2015). Noting this, this study used an experiment (testing), simulation, and scenario to validate the proposed systems. The self-sovereign identity system for the existing electronic healthcare system infrastructures was tested through simulation and scenario using a statistical use model. On the other hand, a decentralized and interoperable health information sharing system for the existing electronic healthcare system infrastructures tested for evaluation using hyperledger caliper version 0.20.8, a performance framework for testing blockchain-based systems.

3.6 Conclusion

The conclusion phase indicates the end of a research project, results of the study are disseminated to show and argue the overall contribution made by the research project to advance knowledge in the research area (Hevner & Chatterjee, 2010; Vaishnavi & Kuechler, 2015; van der Merwe *et al.*, 2017). In this research study, a dissertation was successfully composed and two peer-reviewed research papers that are based on a dissertation were successfully accepted and published in two journals.

3.7 Validity and reliability

Some researchers define validity as the degree to which an assessment measures what it says to measure (Stake, 2010; Golafshani, 2003). It is extremely important that an evaluation is valid so that the results are applied and interpreted correctly. Golafshani (2003) described reliability as the degree of agreement of results over time. The results are said to be reliable if similar findings can be replicated using the same methodology, then it is known that the research tools are reliable.

To assure the validity and reliability of this work, data were collected using various techniques (interviews, documentary review, direct observation, participant observation, and experiments) and from different expertise (healthcare facility leaders, ICT experts, government

representatives, doctors, nurses, laboratory technicians, pharmacists, accountants, and receptionists). This aided to obtain information from multiple angles and, thus, increase the validity of the information.

3.8 Ethical consideration

The researcher got permission from the School of Computation and Communication Science and Engineering at the Nelson Mandela African Institution of Science and Technology, institutions and government authorities for conducting the study in different healthcare facilities in mainland Tanzania (see Appendix 2 and 3). This includes the Regional Administrative Secretaries who introduced the researcher to lower authorities.

The researcher also briefly introduced the respondents about the research objectives and how they are going to benefit from the research (see Appendix 1). The researcher asked permission before using instruments such as cameras during observation, recording during the interview, photos, and narrations from respondents used for the purpose of this study.

The researcher ensured the ethical principles that include respect to the person, privacy, integrity, and confidentiality. According to Berg (2008), ensuring confidentiality is critical if the researcher expects to get truthful and free-flowing discussions during the interview. The researcher ensured that no ambiguities and fear arise during data collection.

3.9 Chapter summary

This chapter presents the methodological procedures for this study. The chapter describes how the study was designed and how it was conducted. The study used design science research (DSR) methodology through its five phases: a) awareness of the problem; b) suggestion; c) development; d) evaluation and e) conclusion. In conducting the study, the researcher observed all ethical dimensions of research to ensure data validity and reliability. Data collection and interpretation was free from the researcher's influences in order to maintain ethical dimensions, data validity, and reliability.

CHAPTER FOUR

RESULTS AND DISCUSSION

4.1 An overview

This chapter presents the results and discussions of the study. The data collection, data analysis, and system design were performed according to the specific objectives of the study along with the research questions. The first objective of the study was to examine the capabilities of the currently available blockchain-based applications for health information systems. The second objective was to analyze the requirements for applicable blockchain-based applications that are best suited to the environment in developing countries. The third objective was the design and development of the proposed blockchain-based system for healthcare providers and the fourth objective was the validation of the proposed system. The results of the first objective are presented in Section 4.2, while in Section 4.3 shows the results of the second objective. Sections 4.4 and 4.5 present the results of the third and fourth objectives, and Section 4.6 discusses the results.

4.2 Assessment of blockchain based healthcare information systems

The assessment of blockchain based healthcare information system was conducted to get an understanding of existing blockchain systems and the requirements for the proposed prototype. This section assesses health information systems in the blockchain ecosystem. The performance monitoring framework for blockchain-based systems was used to assess the three most common blockchain-based healthcare systems. The assessment results were used to determine the requirements for the proposed systems presented in Section 4.4 and Section 4.5.

4.2.1 Blockchain based healthcare information systems

Blockchain is employed in many parts of health information systems; to validate patient data, manage EHRs, monitor research techniques to make safe medications, manage medical financial data, help doctors prescribe, monitor the pharmaceutical supply chain, just to name few (Table 4). Blockchain-based systems in the health sector are classified as: a) public, private or consortium blockchain platforms; b) apply a smart contract or not and c) using a digital token or not. Table 4 shows the properties of some of the health systems currently in the blockchain ecosystem (Kombe *et al.*, 2018).

Table 4: Properties of blockchain based healthcare information systems

BLOCKCHAIN SYSTEM	SMART CONTRACT	BLOCKCHAIN PLATFORM	TOKEN USAGE	APPLICATION	TYPE OF BLOCKCHAIN
MedRec	Yes	Ethereum	No	Medical Data Management	Public
MediLedger	Yes	Ethereum Parity	No	Pharmaceutical Supply Chain	Consortium/ Private
SimplyVital Health	Yes	Health Nexus	Yes	Electronic Healthcare Records	Consortium
Robomed Network	Yes	Ethereum	Yes	Electronic Healthcare Records	Public
Healthureum	Yes	Ethereum	Yes	Healthcare Management	Public
Gem	No	All	No	Patient Data	All
DokChain	Yes	Hyperledger Sawtooth	Yes	Financial and Clinical Data	Consortium
MediBloc	Yes	QTum	Yes	Healthcare Data Platform	Public
BlockMedx	Yes	Ethereum	Yes	Doctor Prescription	Public
Patientory	Yes	Ethereum	Yes	Electronic Healthcare Records	Public
MedicalChain	Yes	Hyperledger Fabric, Ethereum (*for the token*)	Yes	Electronic Healthcare Records	Consortium

4.2.2 Performance evaluation of blockchain-based health information systems

This study assessed three most common blockchain-based health systems chosen from the consortium, private, and public blockchains. The selected systems are Patientory that run on a public ethereum platform, MediLedger on a private parity platform, and MedicalChain on a consortium hyperledger fabric platform. The benchmarking experiment used five metrics, namely network data usage, disk read and write performance, memory consumption, central processing unit (CPU) utilization and transaction execution per time to describe the resource use.

Metrics were selected since assessments of resource utilization and data usage for different systems can be identified and compared. The assessment process was carried out based on experiments conducted using the performance monitoring platform for blockchain (Zheng *et al.*, 2018). Metrics are transactions per disk Input/output (TPDIO), transactions per memory second (TPMS), transactions per second (TPS), transactions per CPU (TPC), and transactions per network data (TPND) (Fig. 5).

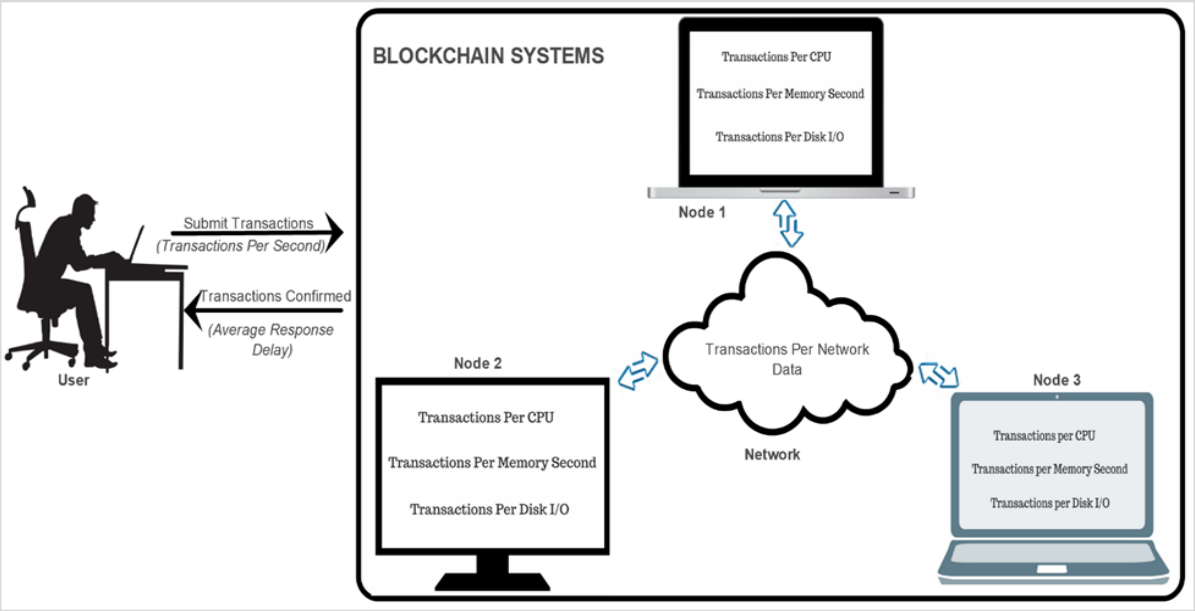

Figure 5: Assessment metrics of blockchain-based health information systems

(i) Transactions per disk I/O (TPDIO)

TPDIO is an indicator used to measure the write and read use of disk storage when executing blockchain systems, such as confirming blocks and executing smart contracts over time. The TPDIO equation for nodes (n) joined to the blockchain system is as follows:

$$TPDIO_n = \frac{Count(Txs\ from\ (t_a,t_b))}{\int_{t_a}^{t_b} DISKR(t)+DISKW(t)}(Txs/kb)$$

(1) (Zheng *et al.*, 2018)

Where t_a and t_b are the time to begin and stop the program execution. DISKW (t) and DISKR (t) are the amounts of data written to the storage and the data read from time (t_a) to time (t_b) in similar storage. The average TPDIO for the entire network with the nodes (N) is:

$$\overline{TPDIO} = \frac{\sum_n TPDIO_n}{N}(Txs/kb)$$

(2) (Zheng *et al.*, 2018)

(ii) Transactions per memory second (TPMS)

TPMS is a metric that represents the use of physical and analogous virtual memory for the transactions of program related to blockchain over time. To compute the TPMS of the node (n) joined to the blockchain system from time t_a to time t_b with a certain number of transactions (Txs), the following formula was applied:

$$TPMS_n = \frac{Count(Txs\ from(t_a,t_b))}{\int_{t_a}^{t_b} PMEM(t)+VMEM(t)}(Txs/(MB.s))$$

(3) (Zheng *et al.*, 2018)

Where PMEM (t) is the main memory employed by the blockchain application from time (t_a) to time (t_b), and VMEM (t) is at the same time the corresponding virtual memory. The average TPMS for the whole system is computed with the formula:

$$\overline{TPMS} = \frac{\sum_n TPMS_n}{N}(Txs/(MB.s))$$

(4) (Zheng *et al.*, 2018)

(iii) Transactions per second (TPS)

TPS is a measure of throughput in a given time that indicates the number of transactions performed by a blockchain system in one second. The time span from t_a to t_b is used by the blockchain application to execute a number of transactions (Txs). TPS of the node (n) in a network, calculated according to the formula:

$$TPS_n = \frac{Count(Txs\ from(t_a,t_b))}{t_b - t_a}(Txs/s)$$

(5) (Zheng *et al.*, 2018)

Hence, the average TPS for (N) nodes is:

$$\overline{TPS} = \frac{\sum_n TPS_n}{N}(Txs/s)$$

(6) (Zheng *et al.*, 2018)

(iv) Transactions per CPU (TPC)

TPC is a measure of CPU utilization when running smart contracts in blockchain networks. TPCs vary from one system to another, relying on the cryptographic algorithms used, hash calculations, and consensus algorithms. Equation (7) demonstrates the formula for computing the node n's TPC from time t_a to t_b:

$$TPC_n = \frac{Count(Txs\ from(t_a,t_b))}{\int_{t_a}^{t_b} F*CPU(t)}(Txs/(GHz.s))$$

(7) (Zheng *et al.*, 2018)

Where F is the frequency of a CPU and CPU (t) is the CPU load of the blockchain system from t_a to t_b. Equation (8) calculates the average TPC for the whole blockchain system with (N) peers:

$$\overline{TPC} = \frac{\sum_n TPC_n}{N}(Txs/(GHz.s))$$

(8) (Zheng *et al.*, 2018)

(v) Transactions per network data (TPND)

TPND is a measure of network flow utilization over a time when a blockchain system shares the status of blocks by transferring data among nodes through the consensus algorithm. This process assures that all system nodes are in the same status.

To compute the TPND in the system, we take time (t_a) to time (t_b) because a blockchain system requires a certain amount of network data flow for given transactions (Txs) in kb. The TPND of a node (n) in a network can be calculated using the formula:

$$TPND_n = \frac{Count(Txs\ from(t_a,t_b))}{\int_{t_a}^{t_b} UPLOAD(t)+DOWNLOAD(t)}(Txs/kb)$$

(9) (Zheng *et al.*, 2018)

Where DOWNLOAD(t) is the downstream network at the time(t) and UPLOAD(t) is the downstream network at the time (t). The average TPND for all nodes joined to the system is computed by the formula:

$$\overline{TPND} = \frac{\sum_n TPND_n}{N}(Txs/kb)$$

(10) (Zheng *et al.*, 2018)

4.2.3 Performance assessment results

The performance experiments executed in blockchain frameworks i.e. parity, ethereum, and hyperledger fabric. Tests were conducted using all kinds of data in a key value database (i.e. CouchDB and LevelDB) through 1000 smart contracts in machines with Intel Core i7-4790 3.60 GHz CPU and 8 GB RAM. The investigated blockchain-based health systems were selected based on their popularity, their blockchain type, and their general functionalities.

These applications are MediLedger on the private parity framework, Patientory run on the public ethereum framework, and MedicalChain on the consortium hyperledger fabric framework (Kombe *et al.*, 2018).

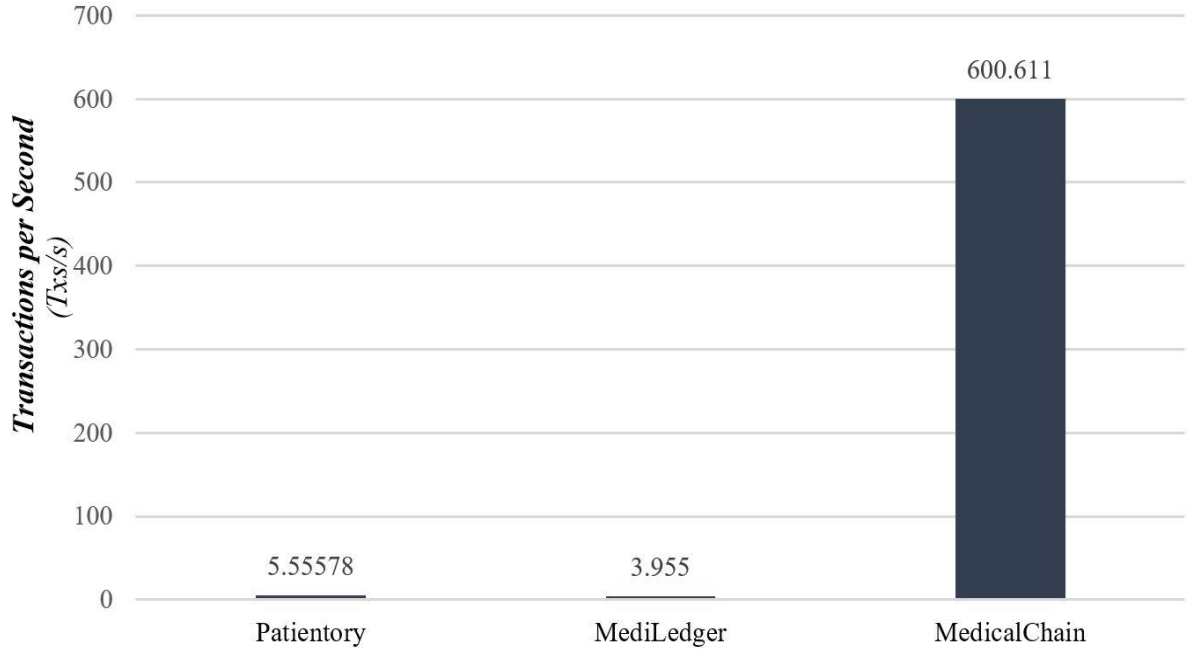

Figure 6: The average transactions per second computed

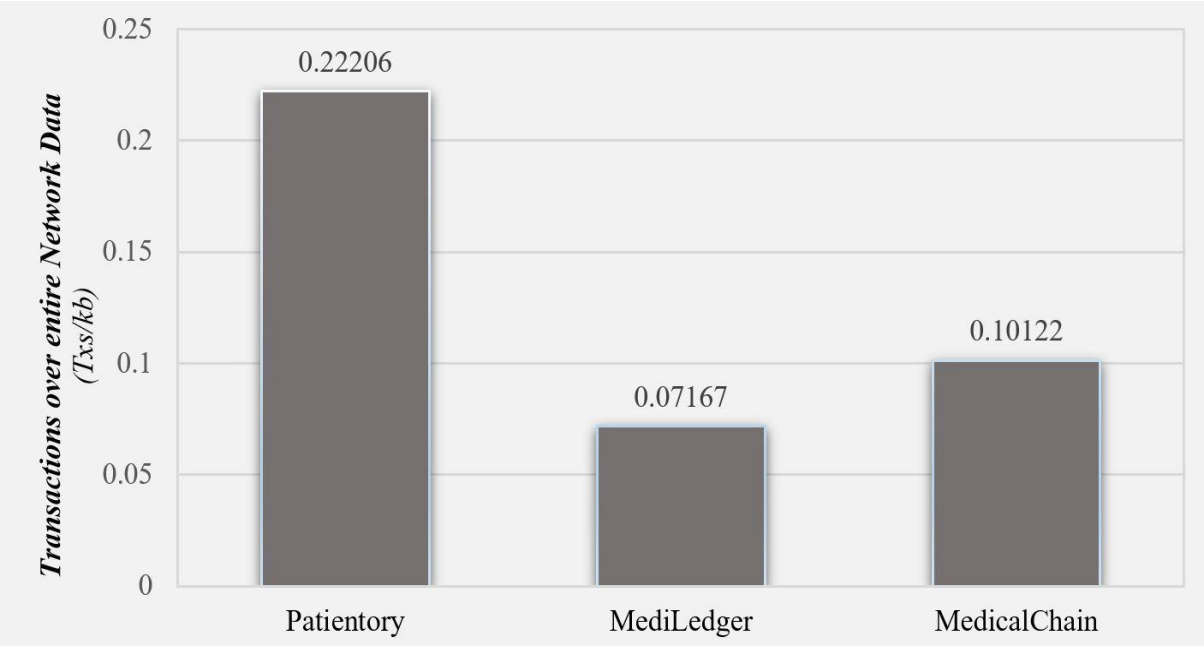

Figure 7: The number of transactions consuming 1 KB per blockchain network data

Figure 6 illustrates the assessment of transactions performed by 3 applications (MediLedger, Patientory, and MedicalChain) to each second. The assessment results showed that the

MedicalChain application runs on a hyperledger fabric performs higher transactions rate compared to MediLedger and Patientory systems.

In addition, Fig. 7 displays the transactions that are computed to take advantage of 1 kb of network data flow in 1 second. These results demonstrated that the Patientory system consumed half the bandwidth of a MedicalChain system. However, the MediLedger system uses twice the bandwidth of MedicalChain and 4 times the bandwidth of the Patientory.

Figure 8: Blockchain system transactions consuming 1 megabyte of node memory per second

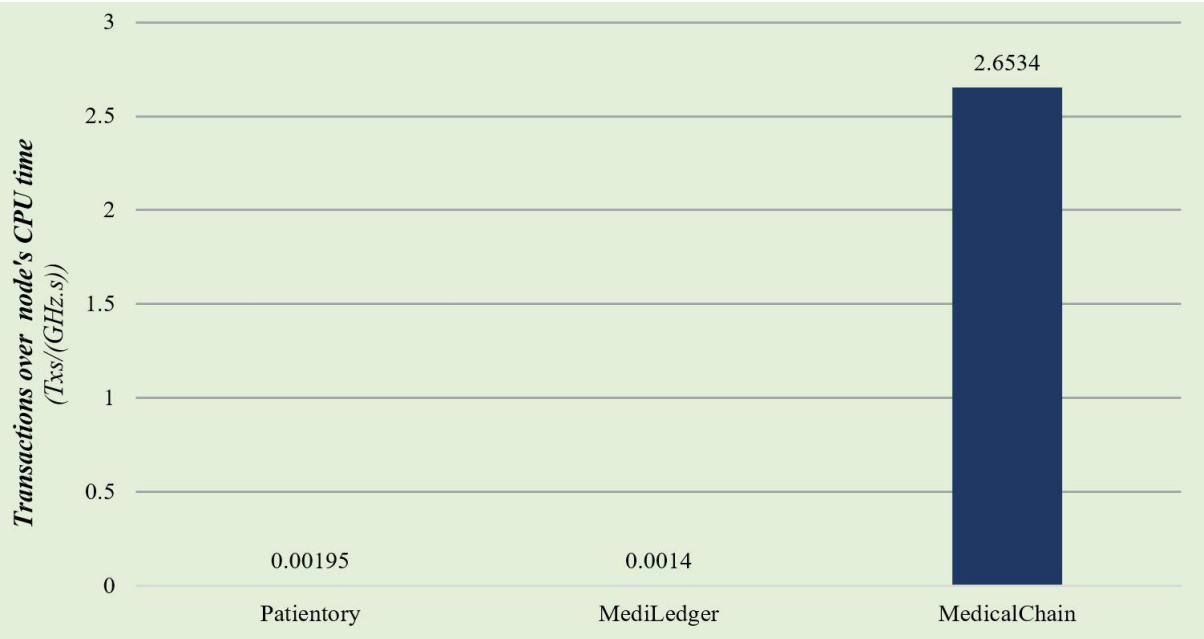

Figure 9: Transactions executed with the blockchain application in CPU cycles per unit time

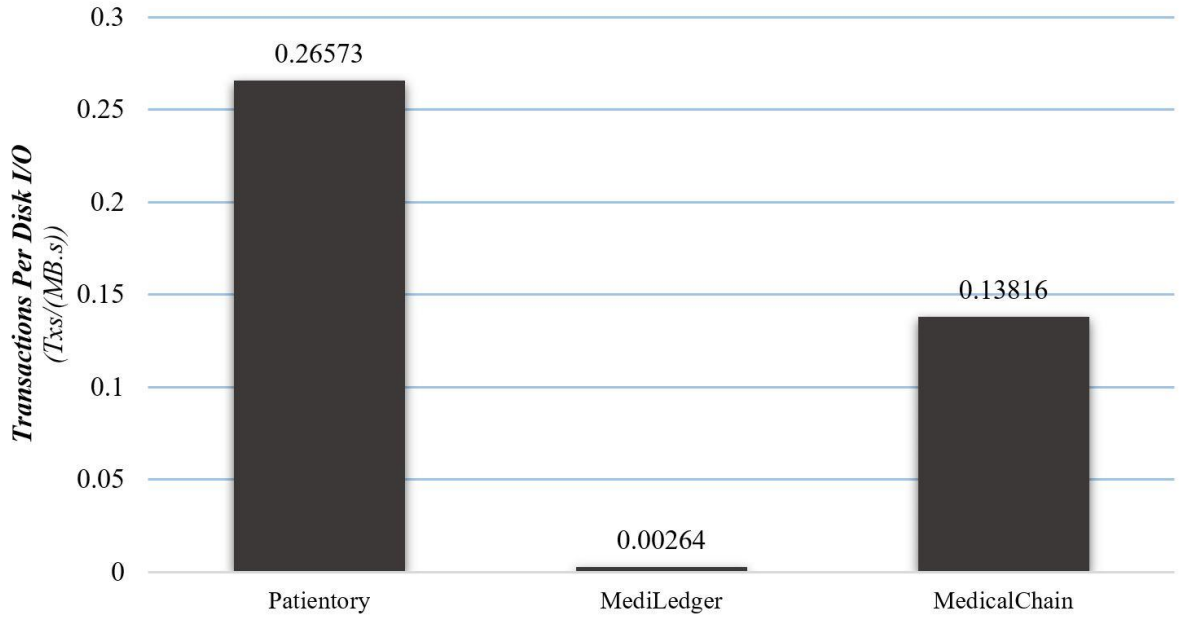

Figure 10: Transactions computed to consume 1 MB of reading and write storage per second

Conversely, Fig. 8 illustrates the transactions that healthcare applications use to consume 1 megabyte of node memory per unit of time. The results demonstrate that the hyperledger-based MedicalChain system uses more than four transactions per one megabyte per second of peer's memory. Moreover, other applications utilized 6.8% and 1.06% of one transaction, correspondingly, to use 1 megabyte per second of machine memory.

Furthermore, Fig. 9 displays the number of healthcare applications transactions utilized to consume one gigahertz processor core per node and unit of time. The results express that the MedicalChain system has finer node CPU performance at 2.6 transactions per 1 gigahertz than the other two systems. Two other systems, (MediLedger and Patientory) used 1.4% and 1.9% of a transaction to utilize 1 GHz.s of a node.

Lastly, Fig. 10 shows the transactions that the healthcare application uses to write and read 1 Mb of data per unit second to/from a node's disk storage. The results showed that the Patientory reads and writes higher transactions for 1 Mb per second than two other systems. It writes and reads 26.57% of 1 transaction for 1 Mb per second. The MedicalChain system has written and read of 13.81% of 1 transaction per 1 Mb per second. The MediLedger system has the lowest writes and reads metrics, with 0.26% of 1 transaction per 1 Mb per second. Therefore, the results demonstrated in Fig. 6 to Fig. 10 were used to determine the proposed blockchain based systems for developing countries.

4.3 Electronic healthcare records systems' problems and blockchain based solutions in Tanzania

This section presents the finding of the second objective. The problems of electronic health systems in Tanzania examined, then the solutions to blockchain-based discovered problems proposed. The findings showed that there are difficulties in handling patients' private data (presented in Section 4.3.2), securely sharing medical information from one healthcare facility to another (presented in Section 4.3.3), and addressing data integrity (presented in Section 4.3.4). Blockchain technology provides solutions to these problems through self-sovereign identity and secure sharing of medical information using hyperledger fabric platforms and systems, and interplanetary file system (presented in Section 4.3.5).

4.3.1 Distribution of hospital information systems with the electronic healthcare records systems in Tanzania

Qualitative data collection methods such as interviews, observations and document analysis were used to collect data from 710 public and private health facilities. Of the 710 health facilities involved, 34.5% have fully implemented EHR / EMR systems. Figure 11 shows the distribution of hospital information systems with the EHR systems from health facilities visited.

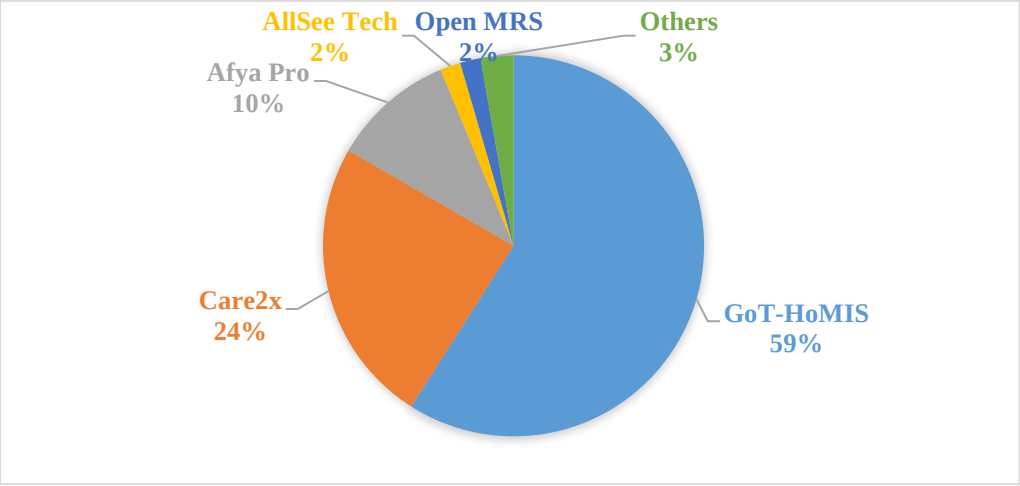

Figure 11: Distribution of hospital information systems with fully installed EHR systems

4.3.2 Privacy issues during the registration process

The patient registration process enables healthcare facilities to collect demographic information, update their tracking details, create clinical records for them, and capture the information required for the billing process (Fig. 12). This process of patient registration offers

many advantages over traditional methods that often involve manual processes. The benefits include enabling quick access to patient records for more efficient services; delivery of more accurate, updated and complete patient records; and above all, to improve productivity with lower operating costs. Despite the benefits mentioned above, the registration process and the mechanism for keeping patient records are affected by security issues related to the privacy and safety of patient data. The existing mechanism allows easy linking of patient records to demographic data, even for unauthorized users. This allows attackers to perform malicious activities such as identity theft and medical fraud.

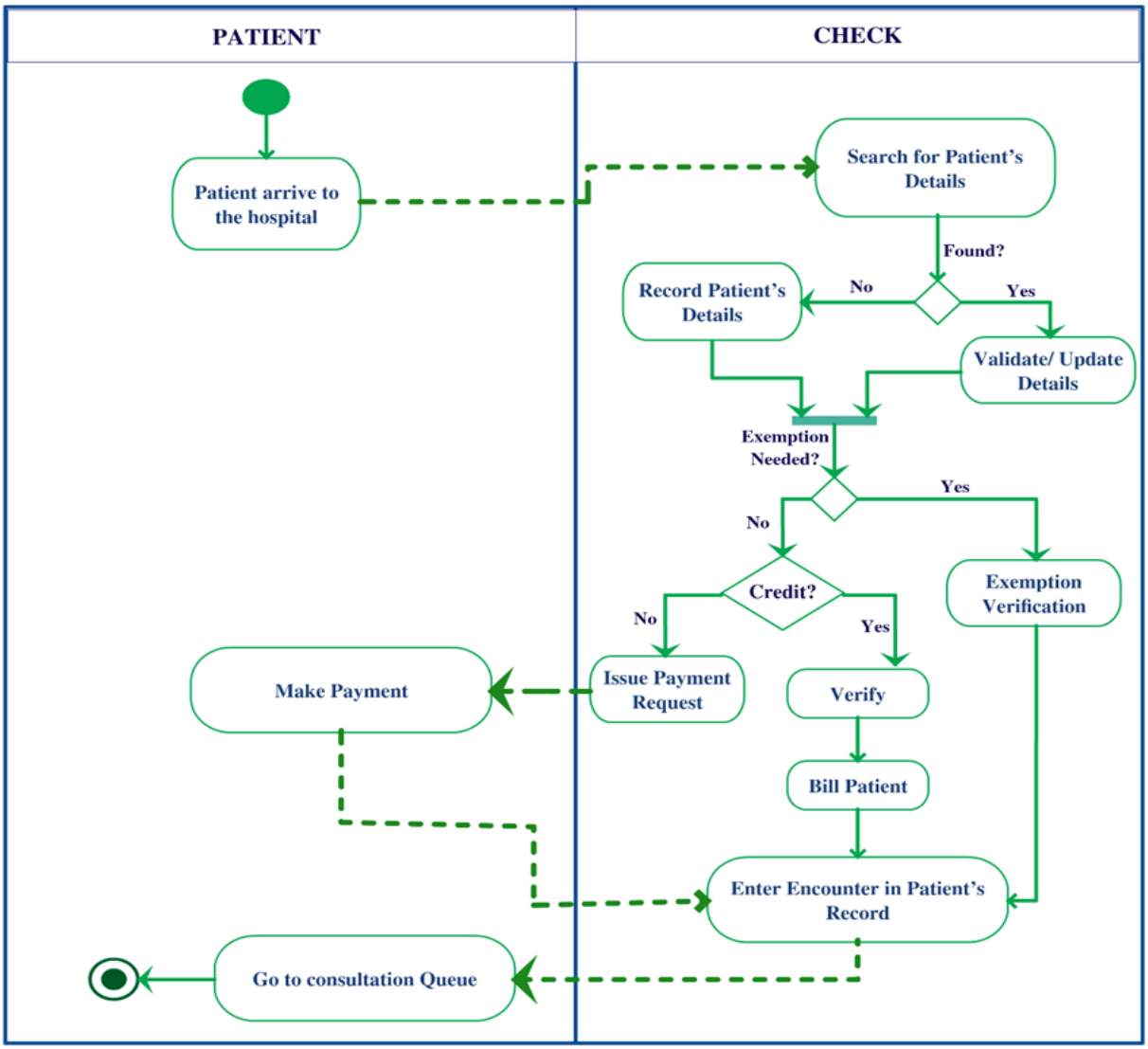

Figure 12: Treatment of patients waiting for consultation

In addition, when asked about the protection of medical images, most system administrators acknowledge that there are no security mechanisms such as encryption and watermarks to protect medical images from confidentiality breaches such as unauthorized access, copying, and modifying medical images that can easily reveal the patient identity or alter patient test

results. Some respondents said they have difficulty in giving researchers access to clinical data because they fear that they will exploit identified and unidentified security vulnerabilities.

4.3.3 Exchange of information between health systems

According to Tanzania national e-health strategy (2013-2018) and Tanzania health sector strategic plan of July 2015 to June 2020, making EHRs system interoperable in Tanzania it is a first priority for the ministry of community development, gender and children (MoHSW, 2013, 2015). Despite of this plan still this study discovered that it is very difficult for a healthcare facility to search, receive, or send patient records to/from another healthcare facility using the EHR system in developing countries environment. This makes it difficult for doctors to reorder tests that have already been done elsewhere. Additionally, the problem can lead to treatment decisions without a complete understanding of the underlying medical conditions or allergies of patients. Currently, it is up to patients or their families to transfer clinical records into printouts from one health facility to another. Proper sharing of patient records helps healthcare providers avoid medication errors, reduce readmissions and avoid unnecessary duplication. On top of individual benefits, record sharing helps to create a complete and holistic picture of the patient, their history, current status, and predictions for the future. The common barrier to interoperability is the appropriate security mechanisms for connecting these systems without allowing unauthorized access. For example, a director of a health facility said:

> *"It is very hard to trust other healthcare delivery institutions with medical records of our patients. Integrating our systems with other systems it is just keeping our systems in jeopardy as you know all these hacking and other malicious activities going on in cyberspace* (Interview with Healthcare Facility Director, 19 March, 2018)*."*

Furthermore, one of the ICT coordinators replied:

> *"Lack of knowledge about secured methods and mechanisms of sharing information and integrating these systems is main problem for interoperability. Also, we lack cyber security staffs who maybe would help us with these integration issues* (Interview with ICT coordinator, 15 February, 2018)*."*

4.3.4 Data integrity

Data integrity in EHRs means a lot to health care providers because they have been used for patient decision making. Therefore, the stored information must be consistent, complete, accurate and up-to-date. Unfortunately, the findings of this study show that some systems are susceptible to vulnerabilities related to data integrity. Most respondents reported issues related to integrity, such as the consistency of information, including modifying and editing information issues, difficulties accessing current information, tracking changes, and patients' medical history. For example, one doctor reacted on the need for proper auditing mechanism:

> *"I'm blocked from seeing accounting details about the prescription I administer to the patients which would help me make right decisions depending on available options and financial status of the patient. Also, I cannot modify the prescription details once I write it to the system* (Interview with a Doctor, 16 February, 2018)*."*

On the other hand, a medical laboratory technician reacted on the same issue with the following statement:

> *"When I make mistake on the system I can't modify. Also, I can't remove wrong test results from the system which affects daily, weekly and monthly analysis reports* (Interview with Medical Laboratory Technician, 20 March, 2018)*."*

In addition, an accountant faced with an integrity problem responded with the following complaint:

> *"Sometimes the system may collapse which leads to loss of financial information which is very important. This problem occurred last year during the system update. After the update, the system showed weird financial figures as in some records indicated excess of amount of money while in other records indicate the loss of money* (Interview with an Accountant, 25 January, 2018)*."*

Additionally, this study observed vulnerabilities related to integrity, such as inadequate data encryption, inadequate data backup, insecure forms of access control, lack of data validation and incorrect tracking of changes. Inappropriate data encryption means that certain information, such as demographic data, is unnecessary for some system users. This means that information such as clinical records or financial details visible to unauthorized users can attract malicious activities such as copying, deleting and modifying. Moreover, this study finds that

most of the systems have not implemented any of data encryption mechanisms such as hash algorithms and the Merkle tree that are used to ensure consistency of stored data.

Furthermore, it has been found that some EHR systems do not have adequate data backup mechanisms that are supposed to guarantee a smooth copy and secure archiving of patient data for recovery in case of failure or loss. Most systems observed; data backups are saved in the same location with the original/live data. This can cause a complete loss of data in cases of device malfunctioning or disasters such as fire or flood. Also, unsafe access control is observed in some systems when two or more users use the same login session to make changes such as updating or adding new information to the system. Access control mechanisms cannot track who makes changes or access certain information in a certain period of time.

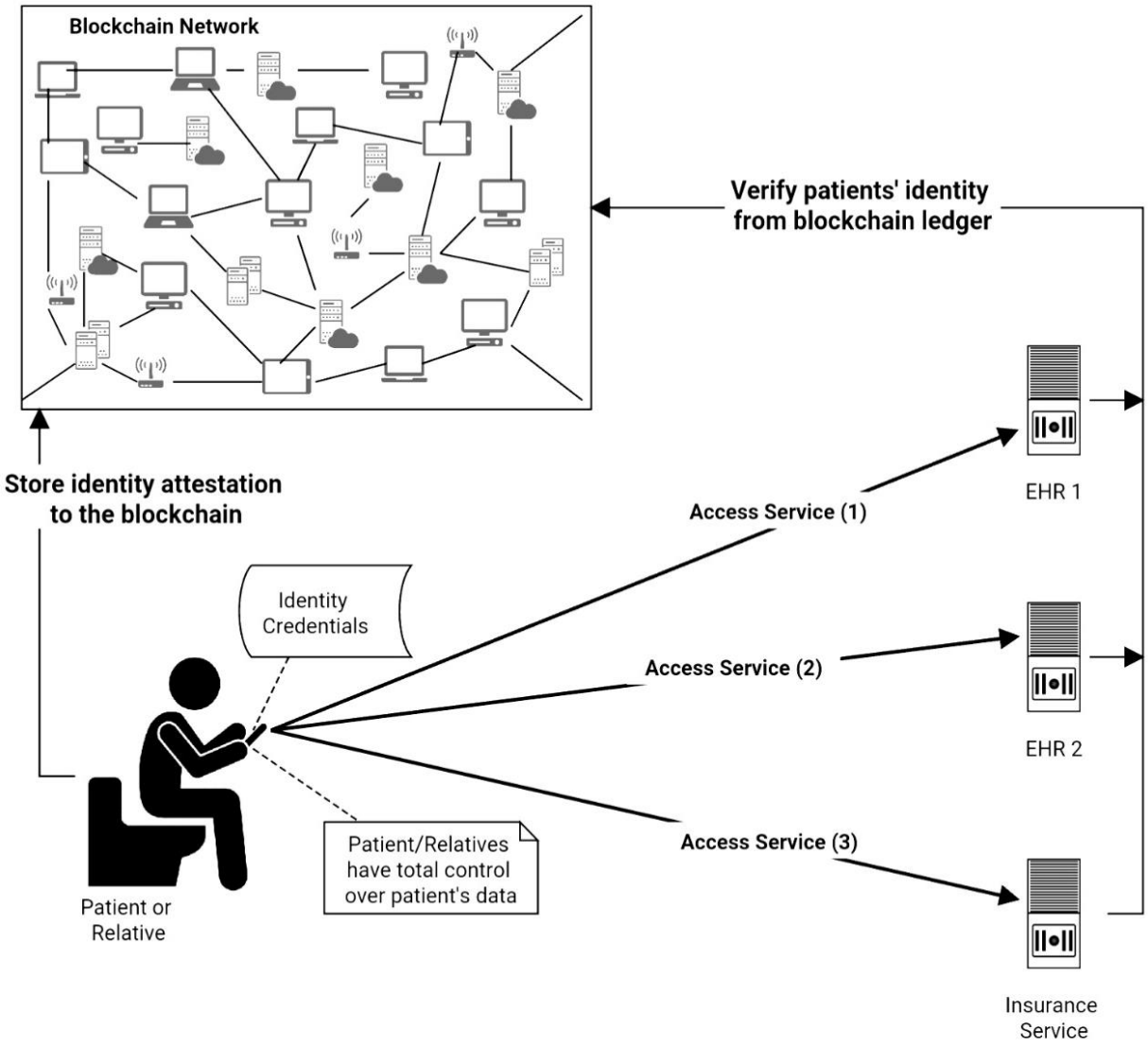

Figure 13: Self-sovereign identity for healthcare information systems

In addition, this study observed that more than 95% of the systems do not have a mechanism to verify the accuracy of stored data while accessing them. Mechanisms such as hash value and the Merkle directed acyclic graph (Merkle DAG) that verify the accuracy of the data accessed was not implemented in these systems. Again, some systems do not allow their users to delete the data or documents entered, but they do not show the proper way to track or locate the different versions of that data or documents or files. Therefore, the situation of healthcare systems indicates that there is a need for more advanced features like blockchain technology's tools to eliminate the weaknesses.

4.3.5 Blockchain based solutions

(i) Blockchain solutions to privacy issues

This study found problems related to privacy in EHR in Tanzania, similar problems also observed in health information systems in South Africa, Kenya and Mauritius (William, 2017). Therefore, to handle the problem, several challenges can be eliminated using blockchain technology such as encryption based on text policy attributes encryption, online machine learning integration with privacy preservation using a private blockchain network, and patient-centred health care data management system that uses blockchain technology as a data warehouse (Al Omar *et al*., 2017; Yi Chen *et al.*, 2018; Magyar, 2018; Wang & Song, 2018; Zhang & Lin, 2018).

However, the best implementation to preserve the privacy of patient information in EHRs is the use of self-sovereign identity (Fig. 13). Self-sovereign identity allows users to control, own, and manage their identity information. Examples of self-sovereign identity systems and frameworks that exist today are ShoCard, Sovrin, Hyperledger indy, and uPort (Domingo & Enríquez, 2018; Dunphy & Petitcolas, 2018; Mühle *et al*., 2018; World Economic Forum, 2018).

(ii) Blockchain solutions to ensure safely sharing patient records between healthcare facilities

The difficulty of safely sharing patient records from one electronic record of medical care to another was also the problem revealed in this study. Also, several studies discovered related problems in their research; For example, Mtebe and Nakaka (2018) revealed a lack of integration between Care2x and HarmoniMD in one of the health care facilities in Tanzania. Furthermore, Kamau *et al.* (2018) presented the lack of interoperability of information between EHR systems in health facilities in Kenya. Since blockchain technology allows digital records

to be shared between different information systems securely and without the need for third parties, it can be used to securely exchange medical information between different EHR systems. The advantages of using blockchain over existing technologies are; its immutable ledger, distributed architecture, and advanced cryptographic security. Currently, blockchain technologies such as hyperledger fabric, ethereum, and hyperledger indy have been used to securely store users' private information off-chain and publicly publish fingerprints in blockchain ledgers. This allows different EHR systems to safely share patient information and verify through fingerprints published in blockchain ledger (Brogan *et al.*, 2018; Dagher *et al.*, 2018; Gordon & Catalini, 2018; Ichikawa *et al.*, 2017; Kombe *et al.*, 2019; Linn & Koo, 2016; Mertz, 2018).

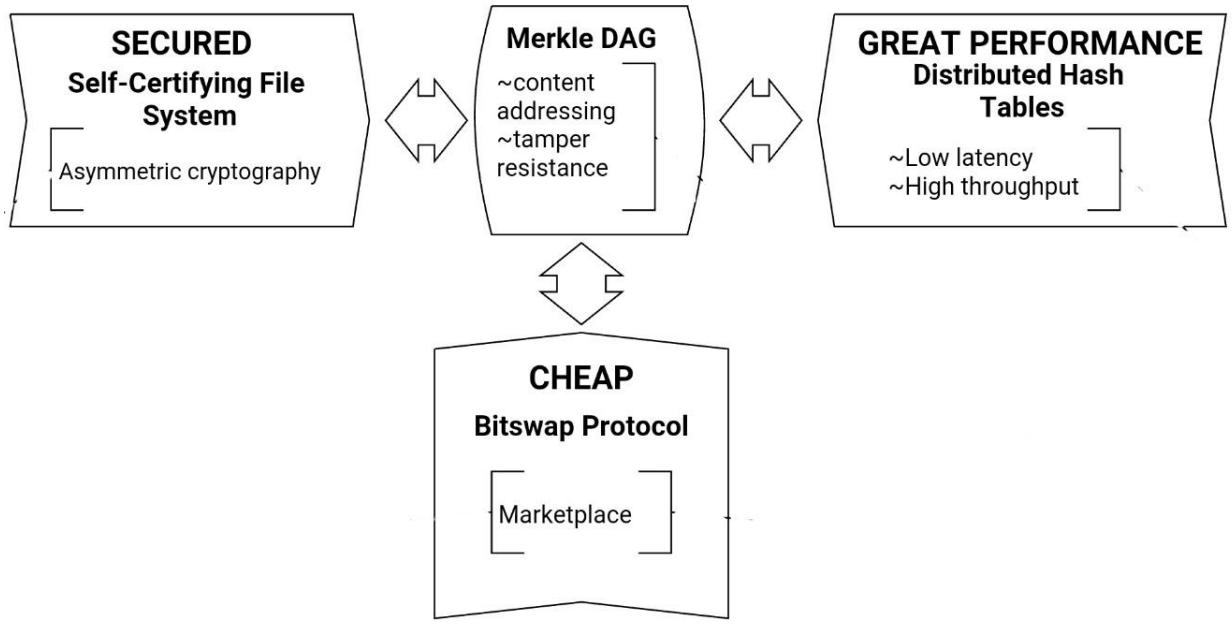

Figure 14: Features of the interplanetary file system

(iii) Blockchain solutions to ensure data integrity

Also, this study revealed that some systems are susceptible to vulnerabilities related to data integrity. Therefore, to ensure data integrity, faster exchange of medical information and, most importantly, the use of low bandwidth, this study proposes the use of the Interplanetary File System (IPFS). Interplanetary File System is the addressed content protocol that is a point-to-point file-sharing system. It includes features such as block exchange, Merkle DAG, Distributed Hash Table (DHT), Self-Certification File System and Version Control System (Fig. 14). These features make IPFS immune to; Distributed denial of service (DDoS) attacks and a single point of failure attacks. For blockchain-based networks, to allow the exchange of large files, IPFS offers a good solution. Through the use of IPFS, users can access their files

from the IPFS nodes where they were encrypted and stored, and the fingerprints of the files are stored in the blockchain ledger for verification (Yongle Chen *et al.*, 2017; Hawig *et al.*, 2019).

4.4 Design of blockchain based self-sovereign identity in existing healthcare systems

Self-sovereign identity is an identity mechanism whereby the identity credential of a system user is owned and controlled by its owner, without the use of external administrative authority through blockchain technology. In existing electronic healthcare infrastructures, as explained in Section 4.3, there is a significant problem in handling private patient data that is stored in digital records. This section designs a self-sovereign identity system that can be integrated with existing electronic healthcare infrastructure to address privacy issues. The hyperledger indy framework is used in a virtualized environment to add self-sovereign identity to two open-source electronic health record systems (Care2x and OpenEMR) on a connected network. Care2x and OpenEMR EHR systems were used because they are open source, widely adopted in developing countries, and the solutions can similarly be adopted to proprietary systems like GoTHOMIS. The system test was performed by simulation using the statistical use model.

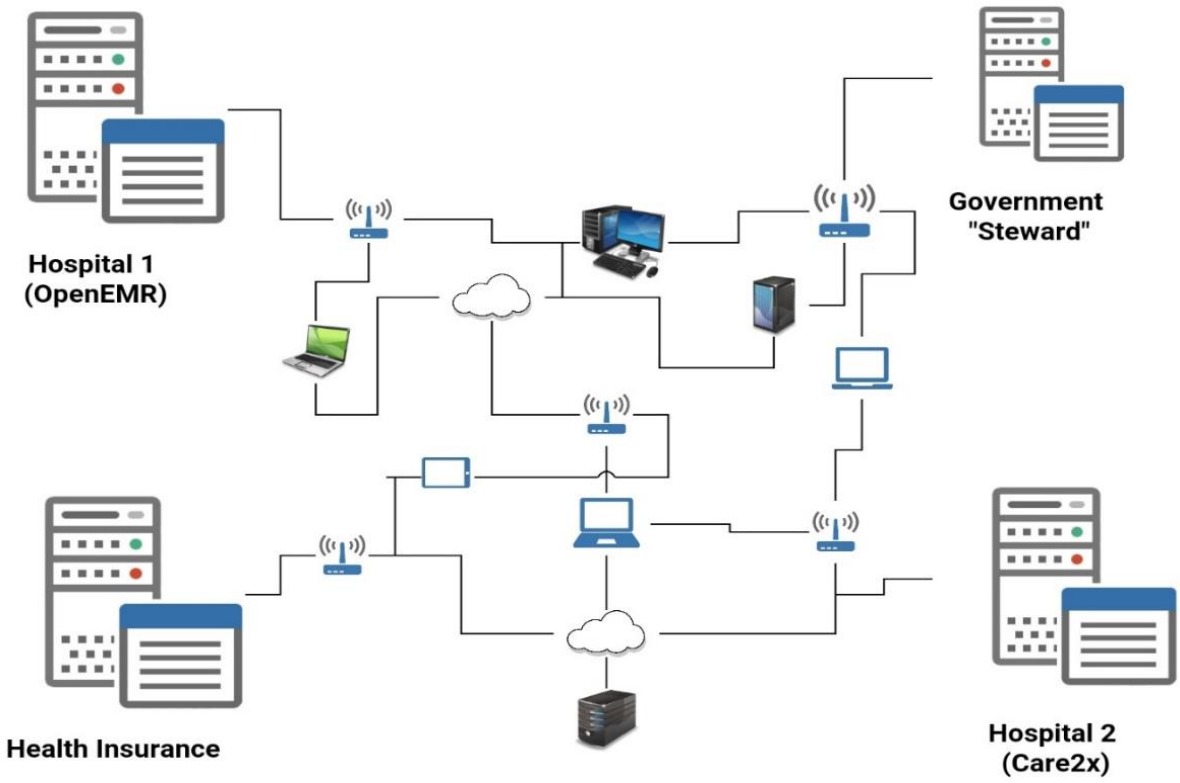

Figure 15: Architecture of the proposed system

4.4.1 Architecture of the proposed system

The proposed implementation will involve hospitals, health insurance and government (Ministry of the country - President's Office Regional Administration and Local Government) that will connect to each other on the computers distributed in the network (Fig. 15).

4.4.2 The setup

The configuration was done in a virtualized environment; four servers were used, two of them with open source EHR (i.e. Care2x and OpenEMR), one with a health insurance database and another with hyperledger indy module used by the Government for identification and providing a trusting anchor role to the other systems. The VirtualBox 6.0.8 version for Linux was used in this design.

(i) Electronic healthcare records

This study used two open-source electronic healthcare records (EHR) systems to integrate with the self-sovereignty system. The systems used are Care2x and OpenEMR (Fig. 16). The Care2x system integrates different types of service, system, department, clinic, process, data and communication in a hospital. Apply the normal SQL database format to store and access data. Care2x is web-based and can be configured to serve multiple database configurations to increase data security and integrity. This study uses the Care2x version 2.7.

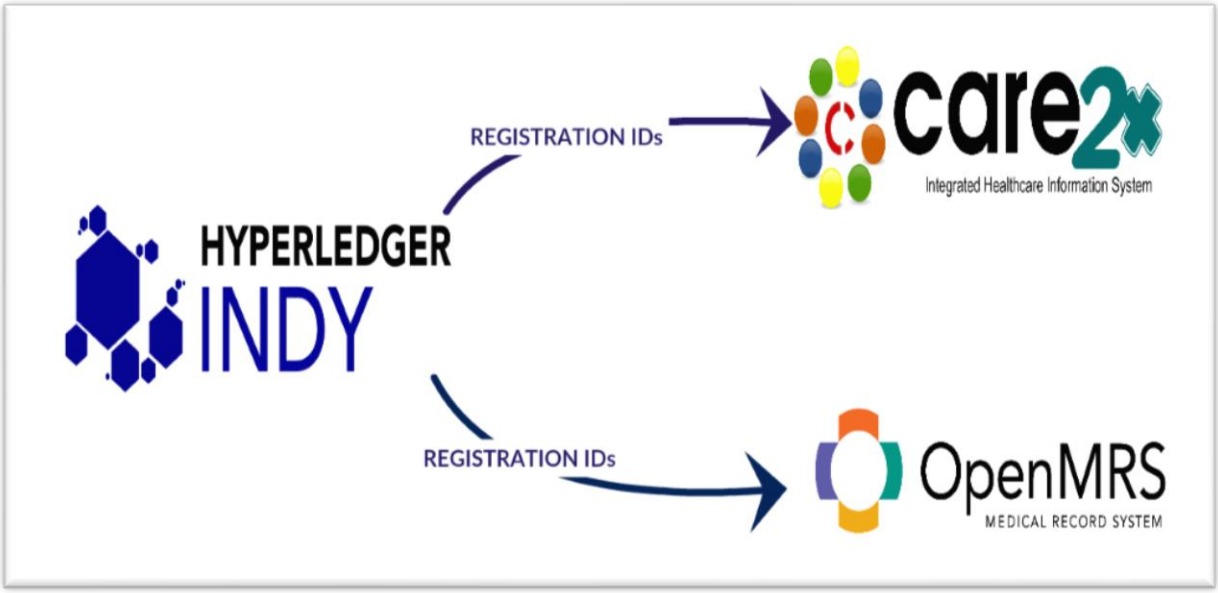

Figure 16: Integration of hyperledger indy with electronic healthcare records systems

OpenEMR is another used open-source medical management software that also coordinates electronic medical records, programming, and electronic billing, as well as maintaining a

history of patient encounters, patient history records, diagnoses, and prescriptions. OpenEMR is one of the most used electronic health system solutions in the world, mainly in developing countries. This study uses the OpenEMR version 5.0.1.

(ii) Hyperledger indy

Hyperledger indy is an open-source identity blockchain framework that provides everyone with self-sovereign identity. It includes programming tools and libraries to develop and apply independent digital identities from blockchains so that they can interact across management domains and applications. Because blockchain ledgers are immune to change, it is important that blockchain-based identity use cases carefully examine fundamental components such as privacy, scaling, performance, and the trust model. Because of this case, this study uses libindy 1.4 to develop a self-sovereign identity tool for existing EHRs. Figure 17 shows the installation of libindy tools for the proposed system.

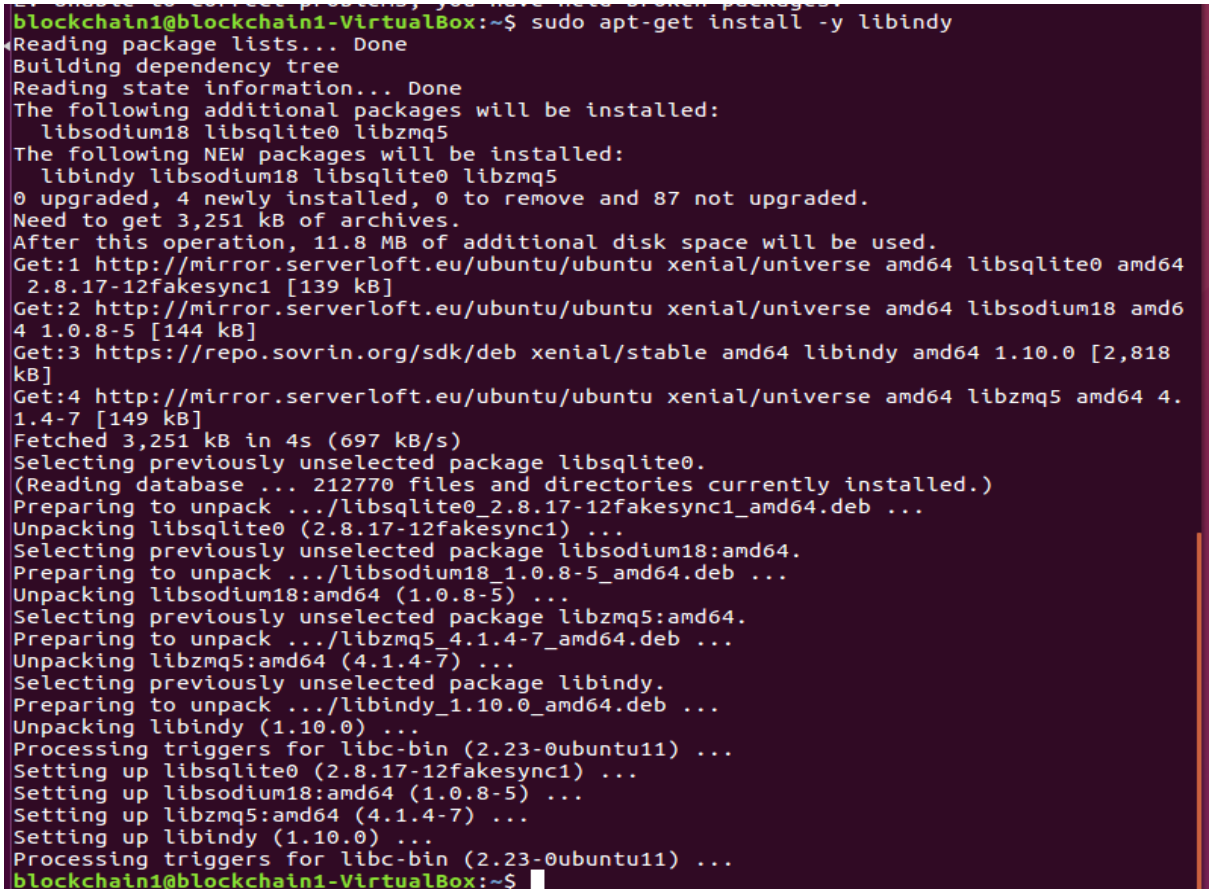

Figure 17: The installation of libindy tools for the proposed system

4.4.3 Requirements specification of the system

The requirements specification is a critical part of electronic system development; It defines functional and non-functional requirements. Function requirements specify the functions that

a system or component must perform. Non-functional requirements measure standards that can be used to assess the operation of a system rather than specific behaviour. This section describes the functional and non-functional requirements of the proposed system.

(i) Functional requirements

Functional requirements relate to certain functions, tasks or behaviours that the developed system must perform. This section lists the key functional requirements for the proposed system. Table 5 summarizes the functional requirements required by the system.

Table 5: Functional requirements of the proposed system

	Requirement	The issue to be addressed
1.	The system shall store the patient and insurance schemas and not the private data to the hyperledger indy blockchain	Revealing the private information of users to unconcerned parties
2.	The system shall store patient and insurance credential definitions to the hyperledger indy blockchain	To let every system user know what exactly is needed by system owners avoid keeping unnecessary private data.
3.	The system shall allow systems owners (insurance company and hospitals) to create credential offers to the patients	Let system owners use private information of patients only when they need it and with patients' knowledge.
4.	The system shall allow system owners to verify the proof of identity of patients through the blockchain	System owners through the digital signature of government (steward), patient, and other system owners stored in the blockchain can be able to verify the identity of the patient without getting to know every detail.
5.	The system shall allow patients to store their own identity information to their own wallet backed by their private keys	The user will have control of their identity information and be able to share their private data with whom they want

(ii) Non-functional requirements

Non-functional requirements describe the required attributes or capabilities of the developed system. They set constraints on the system being developed and postulate external constraints that the new prototype must meet. This section describes the main non-functional requirements for the system.

Security

The proposed system takes care of very sensitive data; protection is therefore very important. The system was developed using a hyperledger indy framework, which contains very powerful

and state-of-the-art cryptographic tools. Preservation of privacy and privacy through design techniques and technologies are the first priorities in self-sovereign identity and, above all, in the proposed system.

Environment

The proposed system runs in any environment that supports a web browser. In addition, it runs on mobile and desktop platforms. The server-side environment is not a client problem and can be updated/changed without affecting clients.

Availability

The system is related to the blockchain nodes that are distributed in nature. Blockchain information guarantees 99.9% availability. This is because the same copy of the information is stored on thousands of computers.

4.4.4 Design of the proposed system

The proposed system was designed using UML diagrams through which use case, sequence, and activity UML diagrams applied to demonstrate the system. The system consists of an actor known as trust anchor; the entity recognised in a blockchain ledger. The proposed system used "Government" as a trust anchor with steward role to create and grant a trust anchor role to hospitals and insurance institutions. The actors with trust role have the ability to create and issue credential schema and credential definition.

A credential schema defines the format and structure for the identity information i.e. names, age, and other identity information. On the other hand, credential definition contains issuer's info (trust anchor), credential schema, and cryptographic keys to verifies the proof of patients' existence. The patient's credentials which sometimes are needed to be filled in credential definitions for verifying the proof of existence are stored in a patient's cryptographic storage called a wallet. Figure 18 to Fig. 20 illustrate UML diagrams for the proposed system.

(i) Use case diagram

The use case diagram demonstrates the relationship between the external worlds and the developed system. The diagram defines a sequence of actions or system behaviour that provides something of measurable value to an actor. In addition, use case diagrams help to recognize the system requirements in depth. The use case diagram in Fig. 18 shows the interaction between the patient, the government acting as steward, the connected EHRs of the hospitals, the insurance system, the proposed system, and the blockchain.

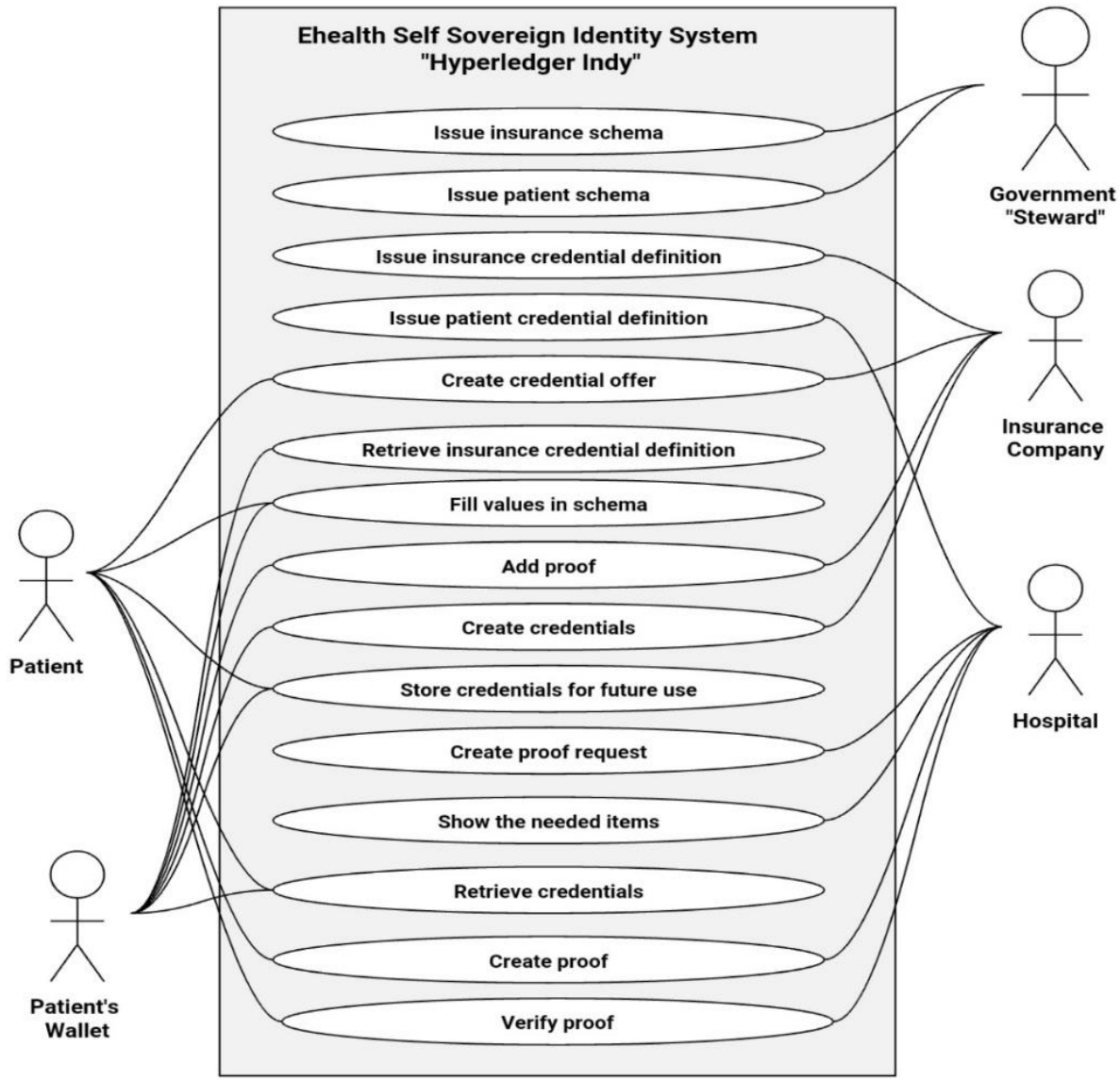

Figure 18: Use case diagram of the proposed system

(ii) Sequence diagram

A sequence diagram illustrates the interactions between objects organized in order of time. They represent objects and classes incorporated in the scenario and the sequences of messages exchanged between the objects necessary to carry out the tasks of the scenario. Figure 19 shows a government that begins to access the system by issuing a schema for hospitals and insurance companies. A schema defines the format of the information that must be completed, such as names, age and other identifying information that must be completed. Then, afterwards, insurance company and hospital issue credential definition which contains issuer's info, schemas, etc. (Fig. 22 to Fig. 24).

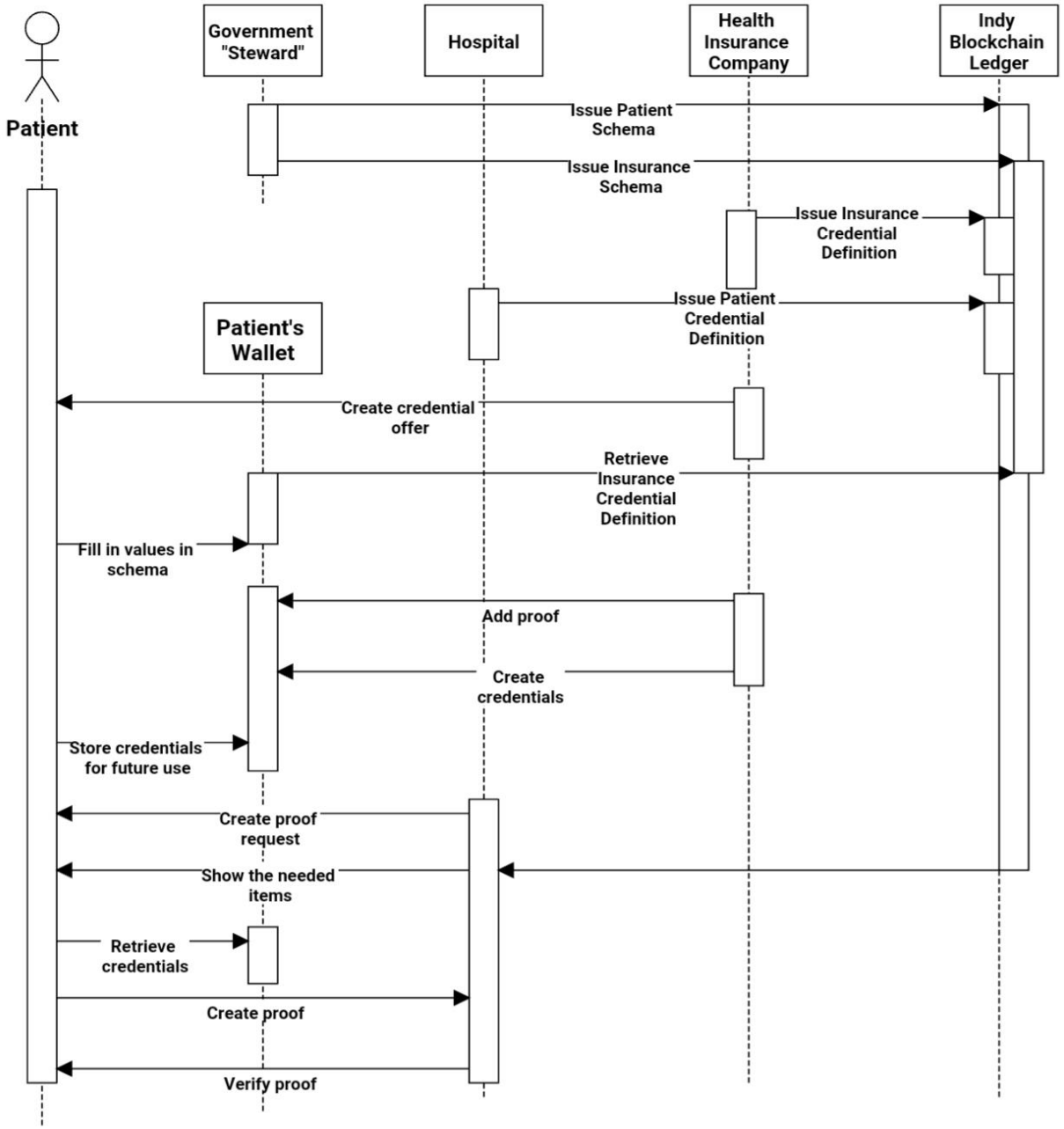

Figure 19: Sequence diagram of the proposed system

(iv) Activity flow diagram

The activity diagram is a flowchart that shows the flow from one activity to another activity. The activity is an operation of the system. The activity diagram in Fig. 20 describes the flow of activities in the proposed system.

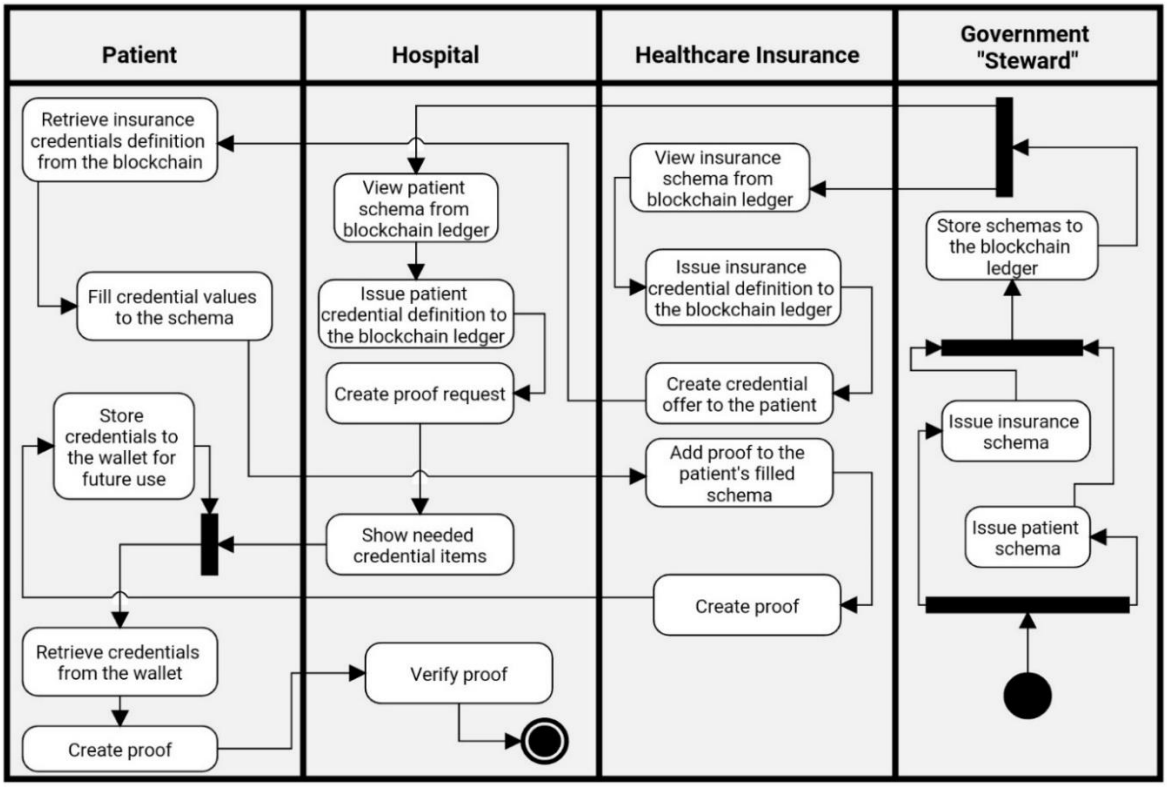

Figure 20: Activity flow diagram for the proposed system

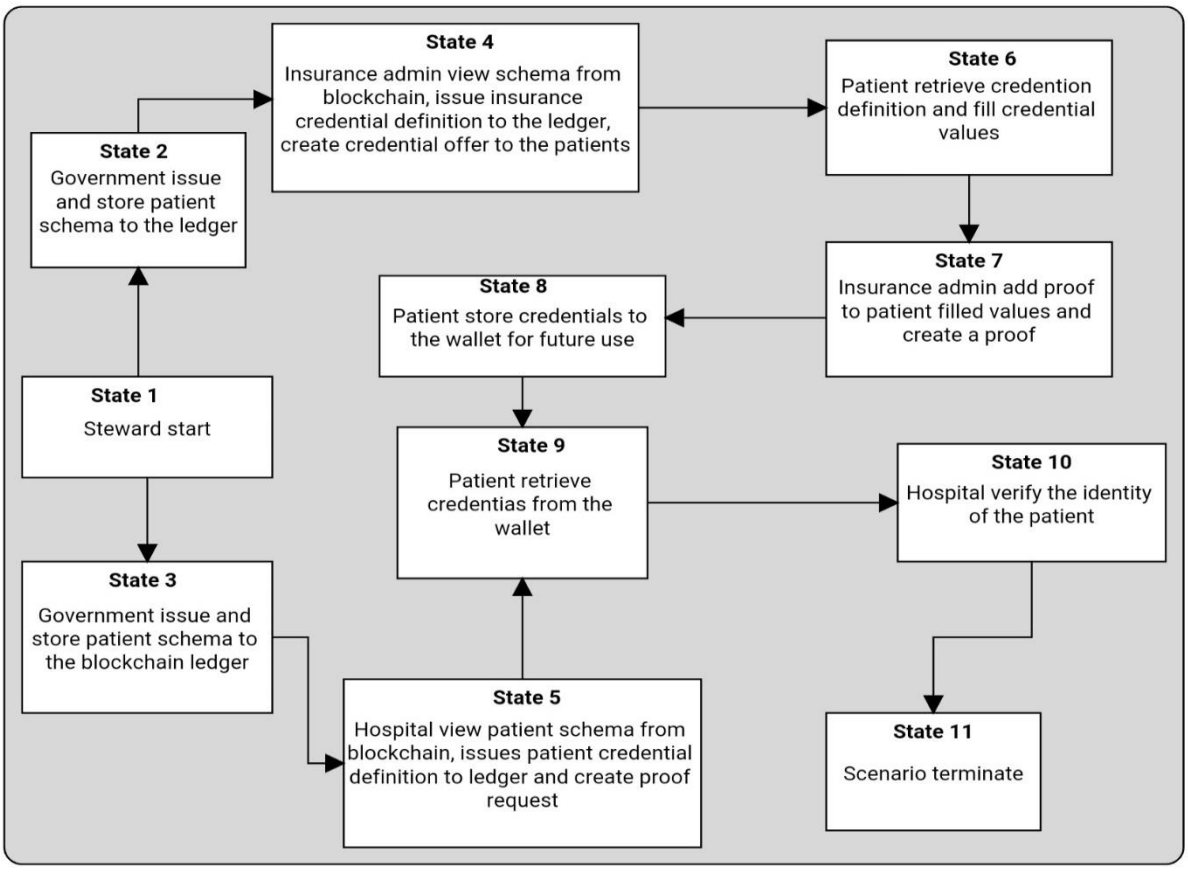

Figure 21: Usage model structure for the proposed system

4.4.5 Testing of the system

The system was tested for verification using a statistical usage model. Statistical usage model is a well-known approach to ensure the correctness of a system by examining its behaviours for a given property. The statistical usage model is simple to implement, understand and cost efficiency (Poore, 1999). Figure 21 presents the transition of states in the proposed system tested indicated in usage model structure. Also, the flow of events was simulated in the virtualized environment (Fig. 22 - Fig. 24) through activities performed by the Tanzanian government acting as a steward, Patient, National Health Insurance Fund (NHIF) system, Arusha Lutheran Medical Centre (ALMC), and Mt. Meru Hospital since testing in a physical is difficult due to sensitivity of healthcare records.

The usage statistics for the proposed system presented in Table 6 through the probability of occurrence of a state to in one sequence of execution and the expected number of a state to occur in one sequence of execution. Figure 22 show how the schema was created while Fig. 23 indicate the creation of credential definition which stored in a blockchain ledger.

Table 6: Usage statistics for the proposed system

State	***Probability of occurrence in 1 sequence***	***Expected number of occurrences in 1 sequence***
1	1	1
2	0.5	2
3	0.5	2
4	1	4
5	1	4
6	0.5	2
7	0.3	2
8	0.2	1
9	0.6	2
10	1	1
11	1	1

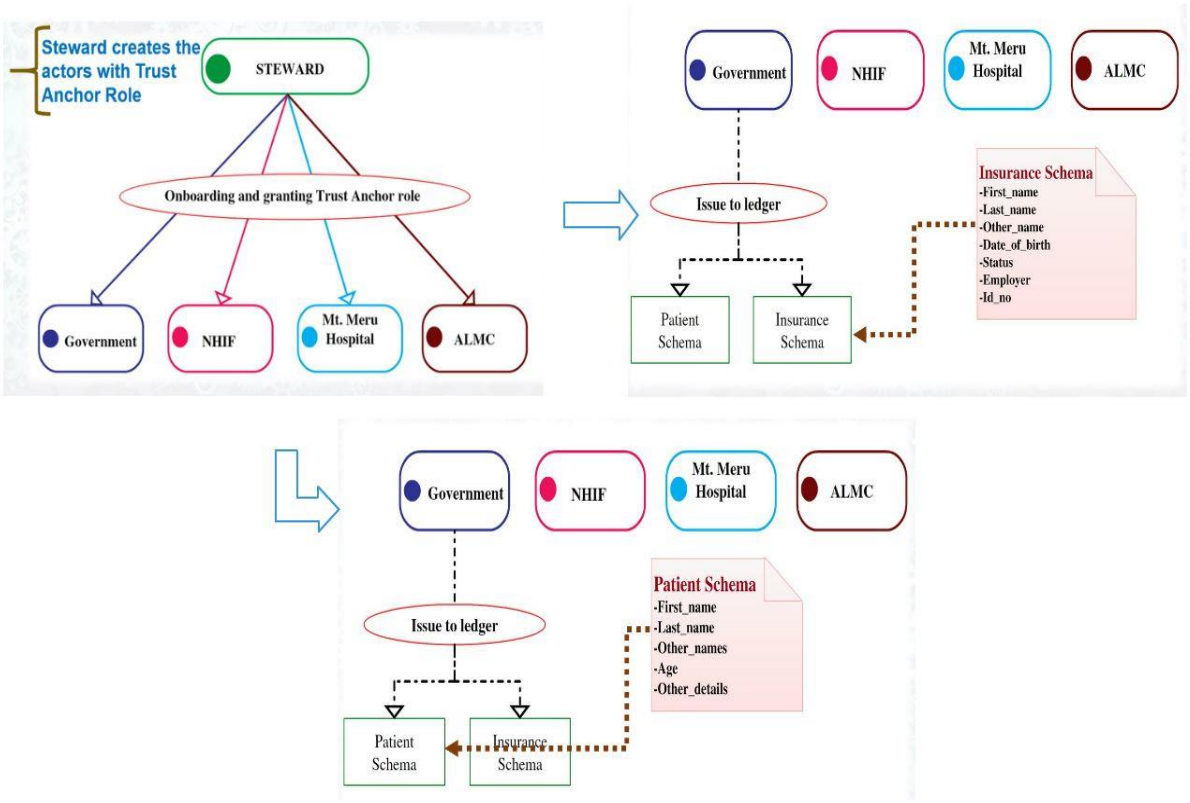

Figure 22: Issuing of schemas to the blockchain ledger by the steward

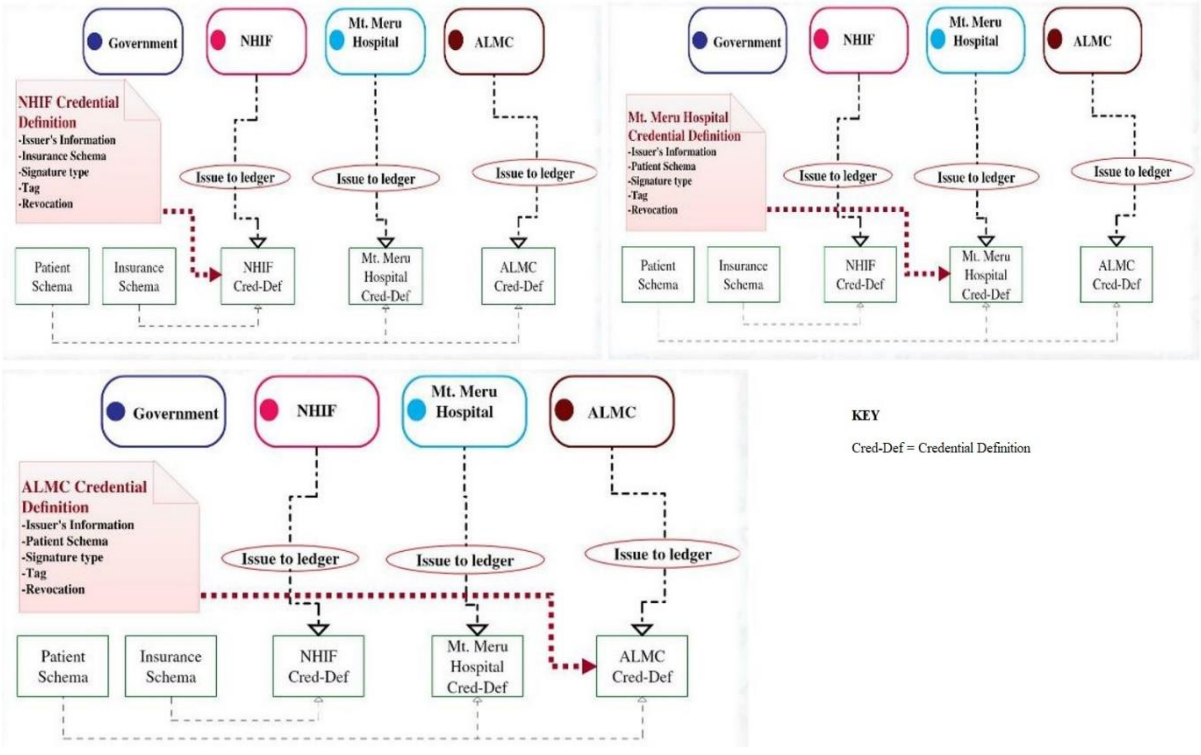

Figure 23: Issuing of credential definitions to the blockchain ledger

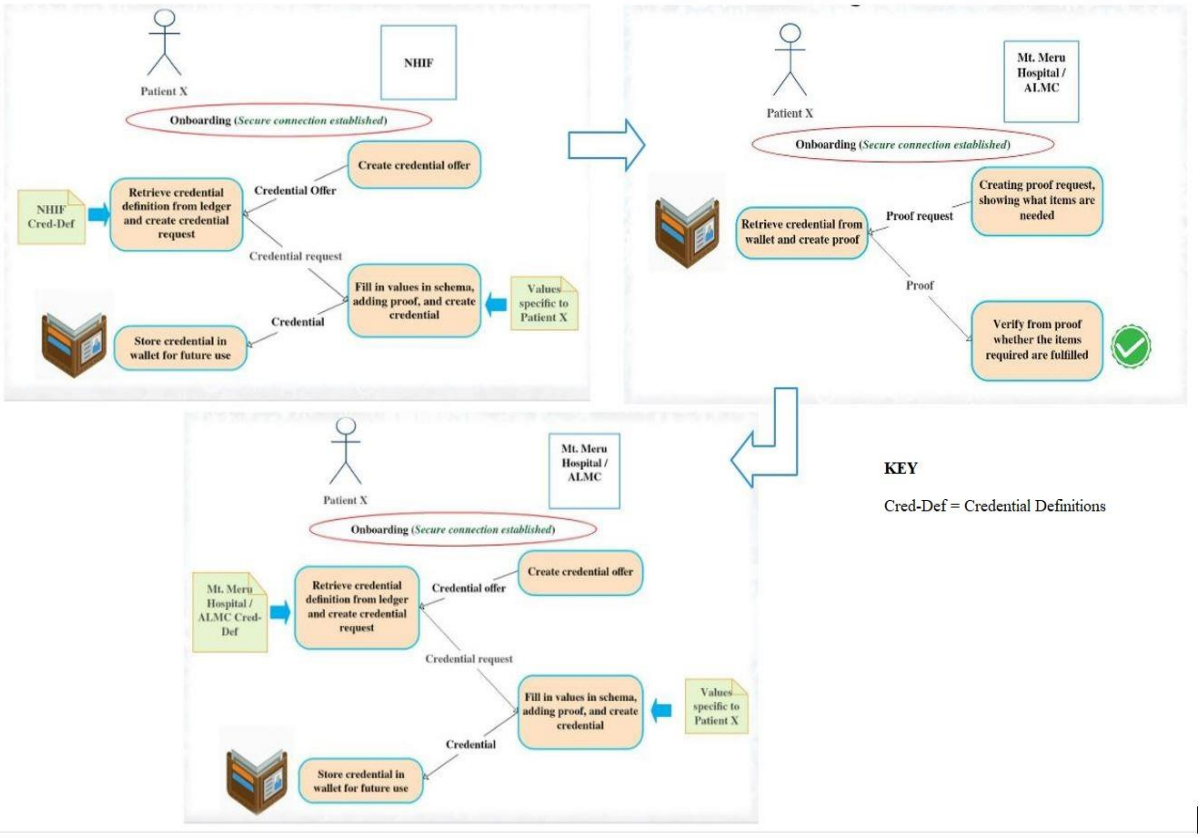

Figure 24: Registering and storing patients' credentials through a secured channel

Lastly, in Fig. 24, which involves patient filling the schema and credential definition through an encrypted channel succeed to store the information in his/her secured account which is protected by a private encryption key (wallet). This helps the patient to store and retrieve information in his/her own secure location and share it without violating privacy.

4.5 Design of decentralized and interoperable healthcare information sharing system

In this section, a decentralized and interoperable healthcare information sharing system with blockchain's advanced security features is designed and developed. The proposed system was implemented on a permissioned hyperledger fabric blockchain framework to allow secure sharing of information between two EHR systems (Care2x and OpenEMR). Care2x and OpenEMR EHR systems were used because they are open source, widely adopted in developing countries, and the solutions can similarly be adopted to proprietary systems like GoTHOMIS. The smart contract for the proposed system developed in JavaScript and, finally, the system tested for evaluation by hyperledger caliper.

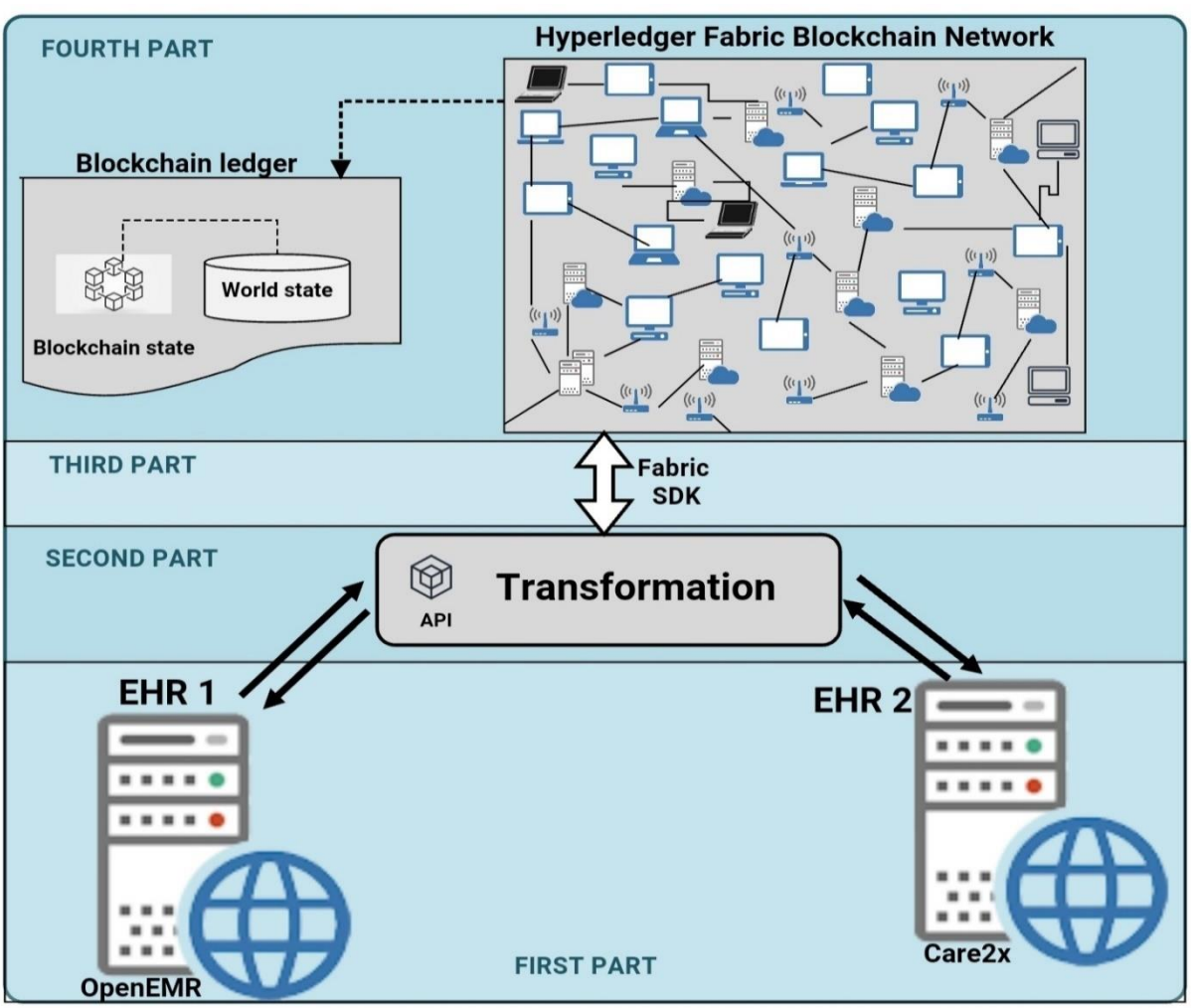

Figure 25: The architecture of proposed healthcare information sharing system

4.5.1 Architecture of the proposed system

The proposed system consists of four main parts (Fig. 25); The first part concerns the existing electronic health record systems of different health facilities. This part may include any number of EHR systems, but two open-source systems, OpenEMR and Care2x, have been used to demonstrate this study. The second part contains the transformation process, in which an application programming interface (API) is implemented to convert the records from the EHR systems into blockchain systems, and vice versa. The records are converted from the SQL format to the NoSQL format. Thus, for this study, since the systems used were OpenEMR and Care2x, the records were converted from a MySQL relational database system to a CouchDB key-value database system and vice versa (Fig. 31).

The third part is the hyperledger fabric system development kit or abbreviated fabric SDK. This part deals with the execution of smart contracts through which the records of the EHR systems are processed and then stored in the hyperledger fabric ledger (Fig. 35 and Fig. 36).

Finally, the fourth part deals with the secure storage of records in the decentralized ledger. The ledger consists of two components: a) the world state to store the instances of healthcare record transactions in NoSQL database format, so CouchDB and LevelDB databases were used for this study (Fig. 32) because they are fast, light and occupy low memory. CouchDB used to store transaction instances and LevelDB to store the activity log and b) Blockchain to store the history of all transactions executed in an immutable data structure format in a file (Fig. 33).

```
Installing Hyperledger Fabric binaries

===> Downloading version 1.4.3 platform specific fabric binaries
===> Downloading:  https://nexus.hyperledger.org/content/repositories/releases/org/hyperledger/fa
bric/hyperledger-fabric/linux-amd64-1.4.3/hyperledger-fabric-linux-amd64-1.4.3.tar.gz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 52.0M  100 52.0M    0     0   311k      0  0:02:51  0:02:51 --:--:--  478k
==> Done.
===> Downloading version 1.4.3 platform specific fabric-ca-client binary
===> Downloading:  https://nexus.hyperledger.org/content/repositories/releases/org/hyperledger/fa
bric-ca/hyperledger-fabric-ca/linux-amd64-1.4.3/hyperledger-fabric-ca-linux-amd64-1.4.3.tar.gz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 6382k  100 6382k    0     0   248k      0  0:00:25  0:00:25 --:--:--  552k
==> Done.

Installing Hyperledger Fabric docker images

===> Pulling fabric Images
==> FABRIC IMAGE: peer

1.4.3: Pulling from hyperledger/fabric-peer
```

Figure 26: The installation of hyperledger fabric framework

```
===> List out hyperledger docker images
hyperledger/fabric-tools       1.4.3               18ed4db0cd57        6 weeks ago         1.55GB
hyperledger/fabric-tools       latest              18ed4db0cd57        6 weeks ago         1.55GB
hyperledger/fabric-ca          1.4.3               c18a0d3cc958        6 weeks ago         253MB
hyperledger/fabric-ca          latest              c18a0d3cc958        6 weeks ago         253MB
hyperledger/fabric-orderer     1.4.3               b666a6ebbe09        6 weeks ago         173MB
hyperledger/fabric-orderer     latest              b666a6ebbe09        6 weeks ago         173MB
hyperledger/fabric-peer        1.4.3               fa87ccaed0ef        6 weeks ago         179MB
hyperledger/fabric-peer        latest              fa87ccaed0ef        6 weeks ago         179MB
hyperledger/fabric-javaenv     1.4.3               5ba5ba09db8f        2 months ago        1.76GB
hyperledger/fabric-javaenv     latest              5ba5ba09db8f        2 months ago        1.76GB
hyperledger/fabric-zookeeper   0.4.15              20c6045930c8        6 months ago        1.43GB
hyperledger/fabric-zookeeper   latest              20c6045930c8        6 months ago        1.43GB
hyperledger/fabric-kafka       0.4.15              b4ab82bbaf2f        6 months ago        1.44GB
hyperledger/fabric-kafka       latest              b4ab82bbaf2f        6 months ago        1.44GB
hyperledger/fabric-couchdb     0.4.15              8de128a55539        6 months ago        1.5GB
hyperledger/fabric-couchdb     latest              8de128a55539        6 months ago        1.5GB
```

Figure 27: The list of installed hyperledger fabric tools in docker containers

4.5.2 Environment setup and configurations

The system was developed and configured in a virtualized environment. Two ubuntu 16.04 operating systems with 4GB of RAM and secondary storage of 30GB each were installed in VirtualBox 6.0.12. The operating systems were named blockchain1 and blockchain 2 and configured on the local area network (LAN) with IP address 192.168.56.4/24 and 192.168.56.3/24, respectively. Care2x 2.7 was installed in blockchain1 and OpenEMR 5.0.1 was installed in blockchain2. Furthermore, the hyperledger fabric 1.4.3 blockchain framework was installed and configured in each of the installed operating systems i.e. blockchain1 and blockchain2. Figure 26 and Fig. 27 show the installation of hyperledger 1.4.3 and its installed docker containers respectively. Docker containers simplifies running and deployment of hyperledger fabric different tools. Figure 28 show how docker was installed in one of the operating system.

After the installation process, the network and consensus protocol configurations followed. For example, Fig. 29 shows the configuration of blocks that are expected to be generated in the blockchain network. In this case, a block is formed by either reaching a timeout of 2 seconds after collecting the first transaction or collecting the maximum number of transactions per block, which corresponds to 10 transactions in this configuration. However, prior to installing hyperledger fabric 1.4.3, there were prerequisites for installations and configurations performed. The programs which were installed and configured as a prerequisite are cURL 7.6.5, Docker 18.09. Docker-compose 1.24, node.js 18.16.0, npm 5.6.0, Python 3, and Visual Studio Code 1.36.0, and all are available for free.

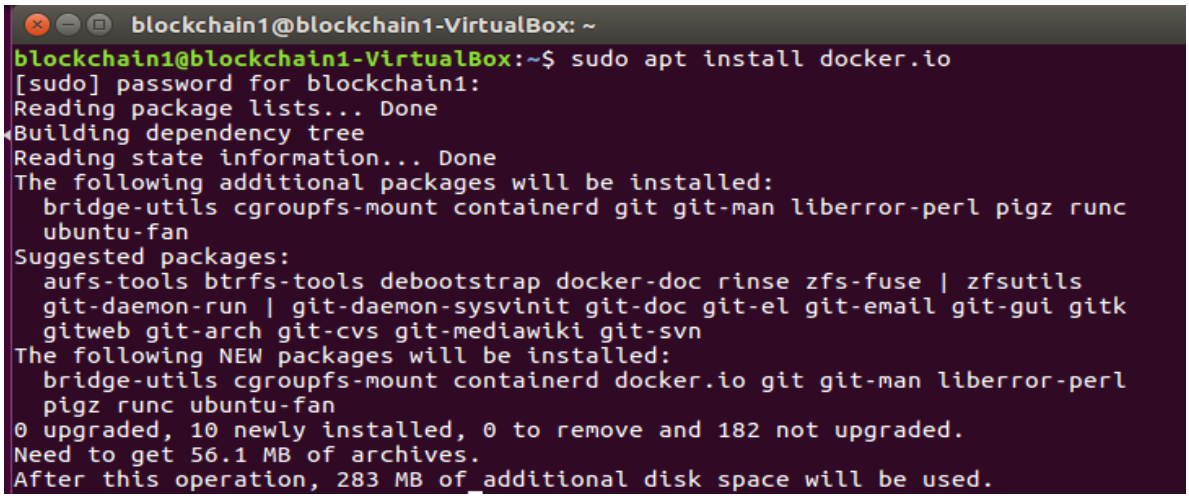

Figure 28: Installation of docker in ubuntu 16.04

```
# Batch Timeout: The amount of time to wait before creating a batch
BatchTimeout: 2s

# Batch Size: Controls the number of messages batched into a block
BatchSize:

    # Max Message Count: The maximum number of messages to permit in a batch
    MaxMessageCount: 10

    # Absolute Max Bytes: The absolute maximum number of bytes allowed for
    # the serialized messages in a batch.
    AbsoluteMaxBytes: 99 MB

    # Preferred Max Bytes: The preferred maximum number of bytes allowed for
    # the serialized messages in a batch. A message larger than the preferred
    # max bytes will result in a batch larger than preferred max bytes.
    PreferredMaxBytes: 512 KB
```

Figure 29: The hyperledger fabric block configuration

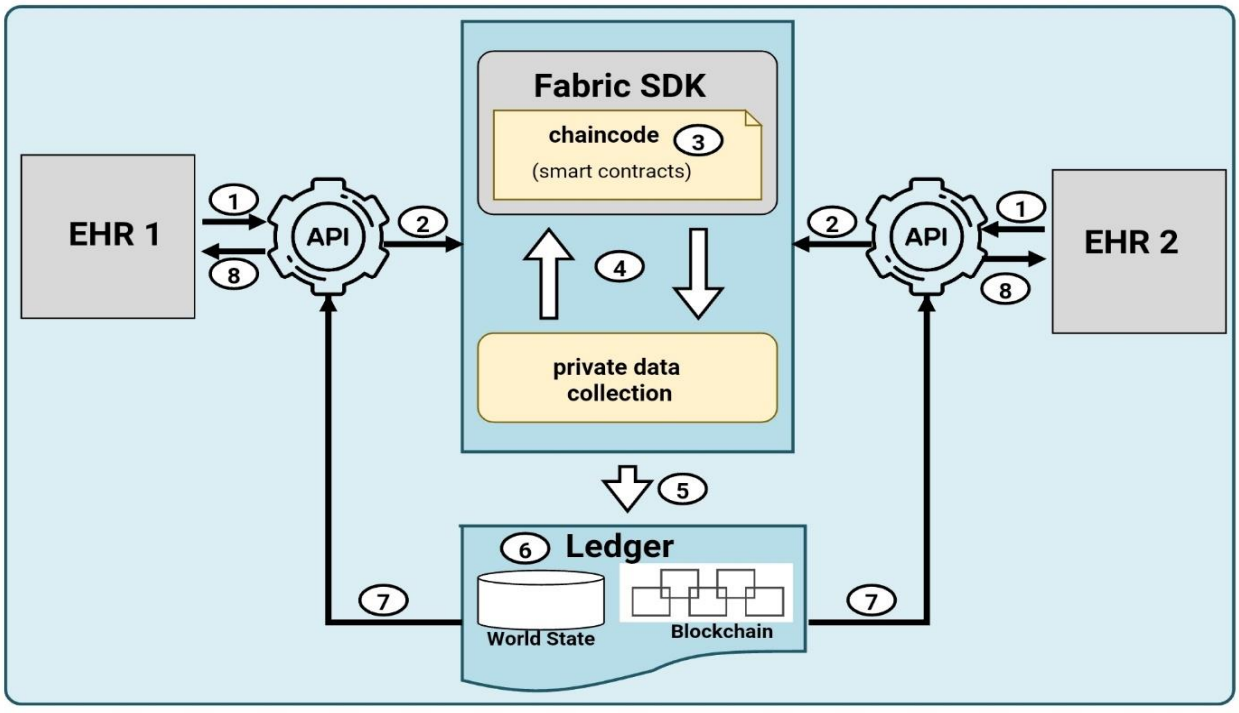

Figure 30: The workflow and components interactions in a proposed system's network

4.5.3 Workflow and system parts interactions

Since the proposed system consists of four parts; EHR systems, APIs, fabric SDK, and ledger, therefore, Fig. 30 illustrates the sequence of actions and interactions of parts as follows: a) submission of records from either EHR systems to API; b) converted records from SQL database to key-value database are submitted to the Fabric SDK; c) the records in a key-value database format are executed in a smart contract; d) records that pose a risk if they are shared,

but must be verified on the blockchain, are securely stored in a private data collection; e) the processed transactions executed in a smart contract are sent to the ledger via the fabric SDK API; f) the processed records are stored in the world state database, and the information and history of all transactions are stored in the blockchain; g) the key value transactions are sent to an API to be converted into SQL records and h) API sends the SQL based records to the either of EHR system.

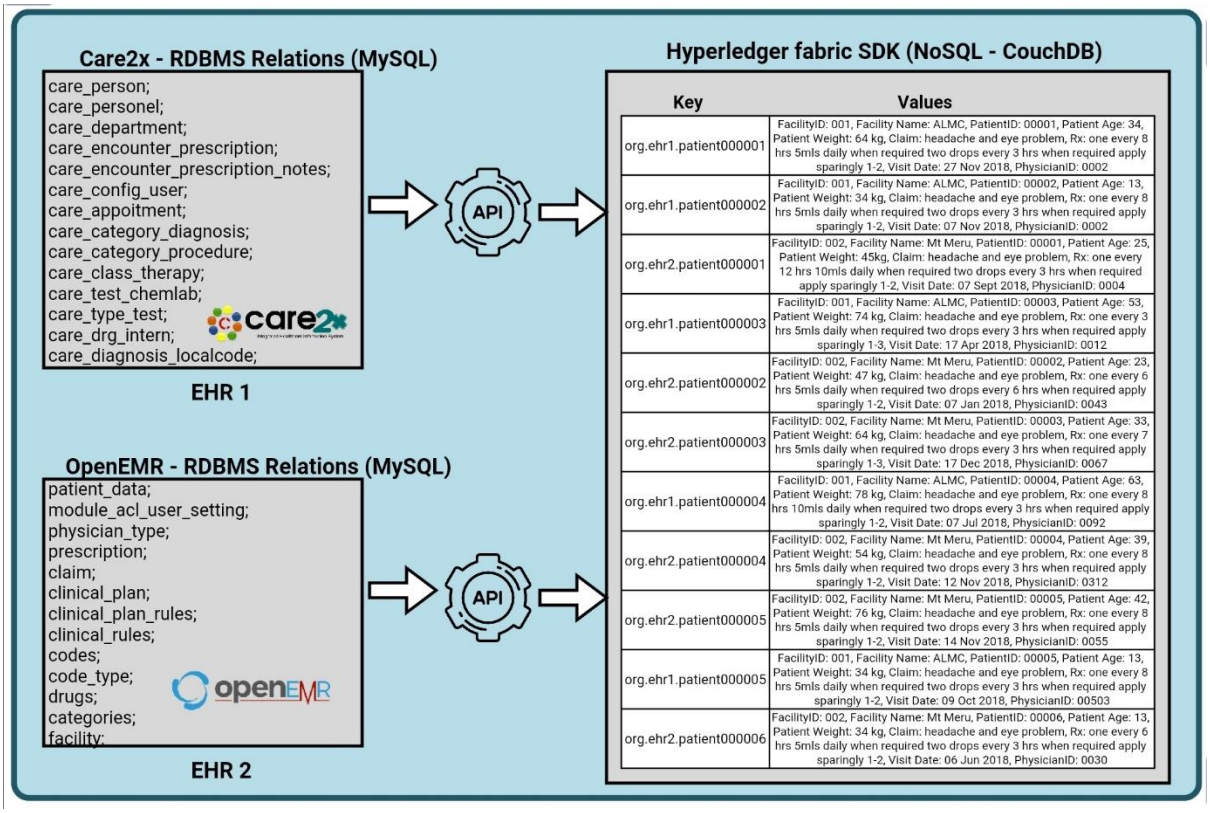

Figure 31: The selection of records from attributes of different relations in RDBMS through the API query

Figure 31 illustrates the selection of records from attributes of different relations in RDBMS through the API query, which is then converted to the key-value database format. In this case, not all records or relations between the EHR systems are shared. The shared attributes are those required for interoperability. Therefore, these attributes are configured in an SQL query by the API.

Figure 32 shows the key-value records and transactions executed in smart contracts in the hyperledger fabric SDK stored in the ledger through Fabric SDK API. The ledger records are stored in two locations: a) the world state database and b) the blockchain. Records in the world-state are stored in a key-value format that includes additional attributes for the version number.

The version number attribute is used to capture the most current version of records in a decentralized ledger.

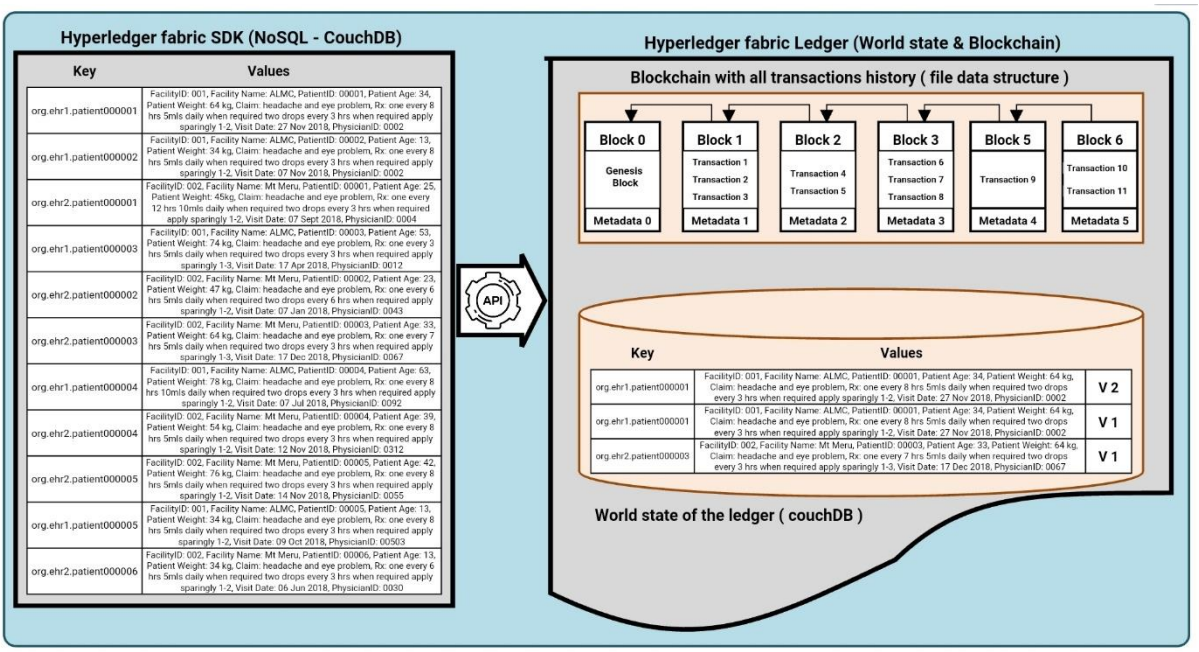

Figure 32: Records and transactions executed in a smart contract in the hyperledger fabric SDK stored in the ledger

The blockchain, on the other hand, stores records differently, here the records and related information of all transactions are stored in an immutable ledger in a data structure format. Figure 33 shows the records that are normally stored in hyperledger fabric blockchains. A block in hyperledger fabric is structured in three parts: a) header; b) list of transactions (data) and c) metadata. The block header contains a block number, the hash value of all transactions listed in the block and the hash value of all transactions in the previous block. All blocks in the hyperledger fabric are structured in this way, except for the genesis block where the hash value of the previous block does not exist. The hash values of the current block and the previous block are used to link the blocks.

The block transaction list part, also called block data, contains the list of all transactions collected in the block. The blocks in hyperledger fabric are usually created in two ways; first, a block is created when the collected transactions reach the maximum number in the required timeline. Second, a block is created after a timeout on a collection of the first transactions. For example, the system proposed in the study has a maximum of 10 transactions and a timeout of 2 seconds from the capture of the first transaction (Fig. 29).

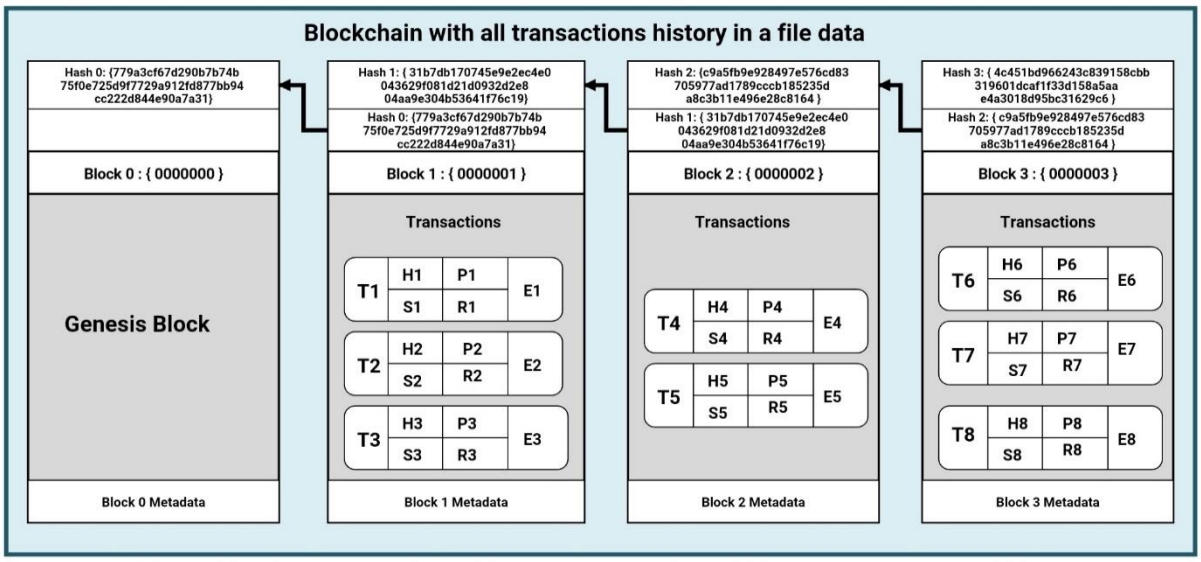

Figure 33: Structure of the blocks for the proposed system

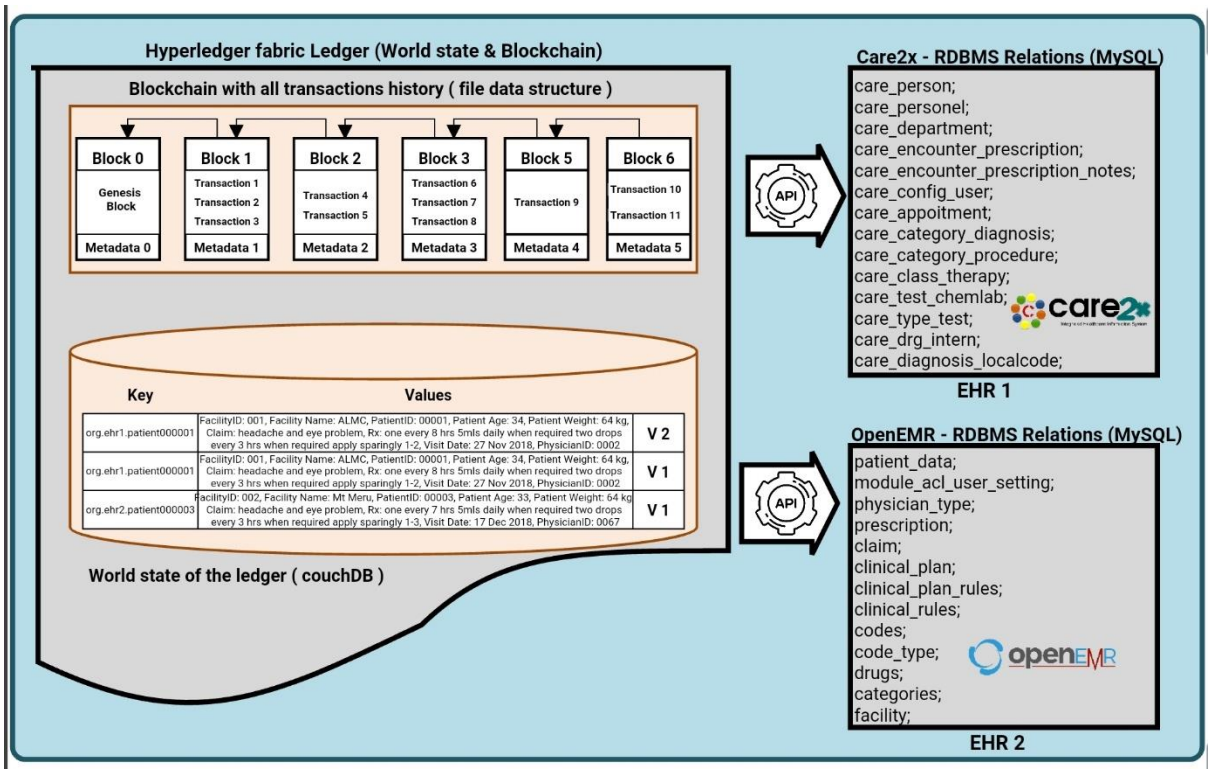

Figure 34: The records in key value format are converted back to SQL relational database through the API queries

Returning to Fig. 33, a transaction in a block resulting from the execution of a smart contract contains the following attributes: a) Transaction signature (S) to ensure the integrity of the transaction; b) header (H) which captures metadata of the transaction like information about the smart contract created the transaction and time of execution; c) encoded input parameters in a smart contract proposed (P) to update the ledger; d) response (R) to record the state of

world state database before and after the execution of transaction in a smart contract and e) the endorsement attribute to record the signatures of the nodes endorsed and validated the transaction. Lastly, the block metadata stores block information such as block creation time, and certificate, signature, and a public key of the node created the block.

Figure 34 illustrates the key value format records that are converted back to the SQL relational database through API queries. The same copy of the ledger is stored in EHR systems; therefore, the conversion process is performed locally on a node where the EHR is installed.

4.5.4 Smart contract and transaction definitions

The smart contract of the proposed system was developed in the JavaScript programming language. The same copy and version of the smart contract are shared between the nodes connected to the network. Figure 35 shows how the smart contract classes were created for the proposed system by extending the default smart contract classes of the hyperledger fabric. The *PatientContext* class was created by extending the default *context* class of the hyperledger fabric. This class represents the context of the transaction (ctx) that holds the information, such as the transaction identifier, the signatures of the transaction, the certificates and how to access the required ledger before the execution of the smart contract and a specific transaction.

```
// Fabric smart contract classes
const { Contract, Context } = require('fabric-contract-api');

/**
 * A custom context provides access to list of all success patients transactions
 */

class PatientContext extends Context {

    constructor() {
        super();
    }
/**
 * Define EHR interoperability smart contract by extending Fabric Contract class
 *
 */
}
class EhrInteroperabilityContract extends Contract {

    constructor() {
        super();
    }
```

Figure 35: Smart contract classes for the proposed system

The *EhrInteroperabilityContract* class, on the other hand, was implemented by extending the default hyperledger fabric *contract* class. This class contains the transaction definition for the transaction (save) represented by the *save ()* method (Fig. 36). The transaction defined by the

save () method sends the records in the parameters to the ledger. The *ctx* parameter represents the transaction context that tracks the information that will be stored in the transactions within the blocks in the blockchain ledger.

```
class EhrInteroperabilityContract extends Contract {

    async save(ctx, facilityID, facilityName, patientID, patientAge,patientWeight,
    claim,prescription,visitDate, physicianID) {

        let ptransaction = EhrInteroperabiltity.createInstance(facilityID, facilityName, patientID,
        patientAge,patientWeight,claim,prescription,visitDate, physicianID);

         ptransaction.setSaved();

         await ctx.patientTransList.addTransaction(ptransaction);

         return ptransaction;

    }
```

Figure 36: The definition of EhrInteroperabilityContract class

Table 7: The test configurations for the proposed system

Name	**Configuration**
Number of test rounds	5
Number of transactions submitted per test round	500 transactions
Transactions rate control	Fixed rate (*100 tps in test 1, 200 tps in test 2, 300 tps in test 3, 400 tps in test 4, and 500 tps in test 5*)
Endorsement policy	2 – of - 2
Network size	2 orgs with 2 peers with CouchDB
Order type	Kafka
Distribution	Multi host
Number of clients	5

4.5.5 System testing and evaluation

The proposed system was tested for evaluation using hyperledger caliper version 0.20.8, a performance framework for testing blockchain-based systems. The performance metrics tested were the success rate of the transactions, the latency of the transactions in seconds (s) and the performance of the transactions measured in transactions per unit of second (tps). The system was tested in five test rounds through which 500 transactions were sent in each round. The transactions were submitted at fixed rates of 100 tps in the first test, 200 tps in the second test, 300 tps in the third test, 400 tps in the fourth test and 500 tps in the fifth test. Table 7 shows a summary of the test settings.

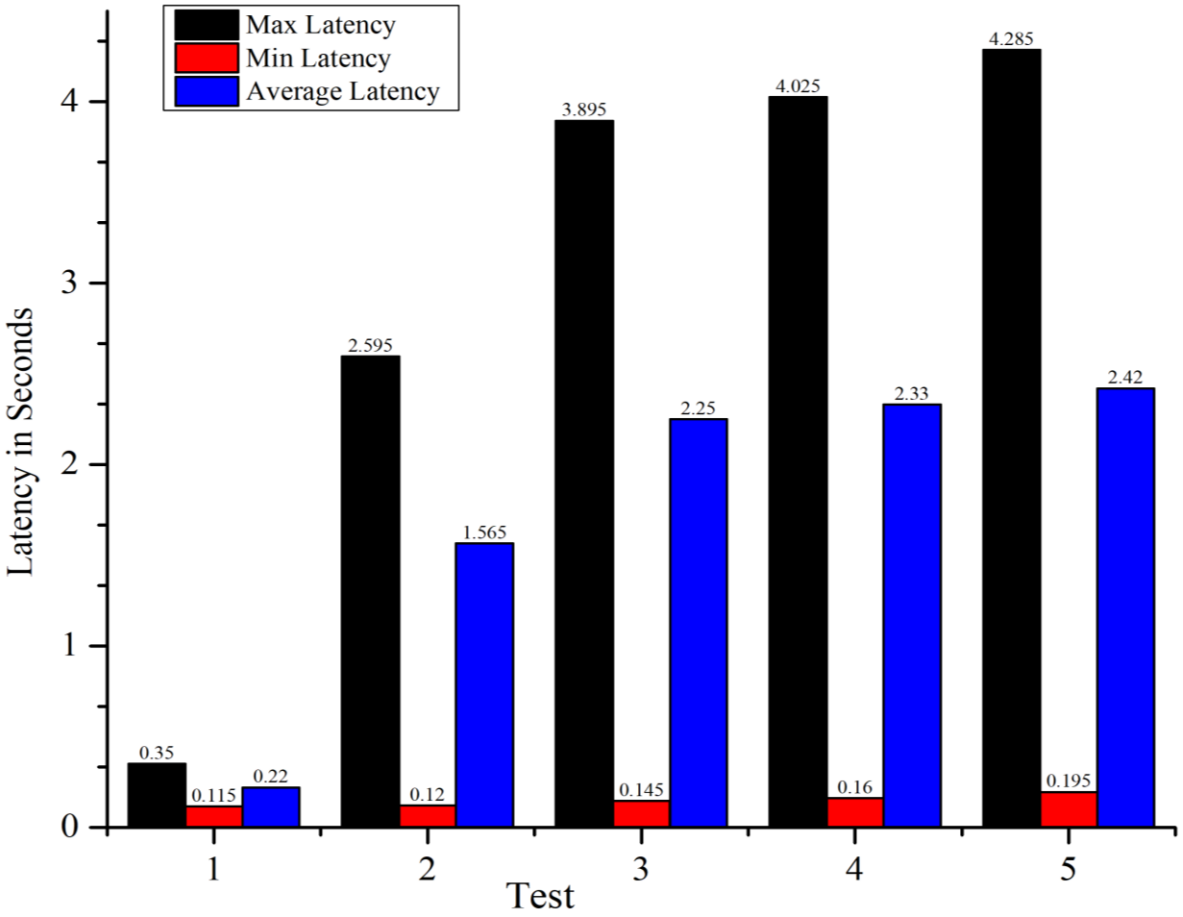

Figure 37: Average transactions latencies per test

The test results showed that for 500 transactions presented in each of the 5 tests performed, all transactions were successful with a 100% success rate. Further, Fig. 37 presents the average latencies were 0.22 seconds for test 1, 1.565 seconds for test 2, 2.25 seconds for test 3, 2.33 seconds for test 4 and 2.42 seconds for test 5, which resulted in an overall average latency of 1.757 seconds and a minimum overall latency of 0.147 seconds. Moreover, Fig. 38 shows the following average throughput; 96.75 tps for test 1, 99.3 tps for test 2, 93.75 tps for test 3, 97.25 tps for test 4 and 98 tps for test 5 with a resulting average transaction throughput of 97.01 tps. Therefore, these results of a 100% transaction success rate, an average minimum latency of 0.147 seconds, the overall average latency of 1.757 and 97.01 tps of average transaction throughput indicate that the proposed system will experience good performance.

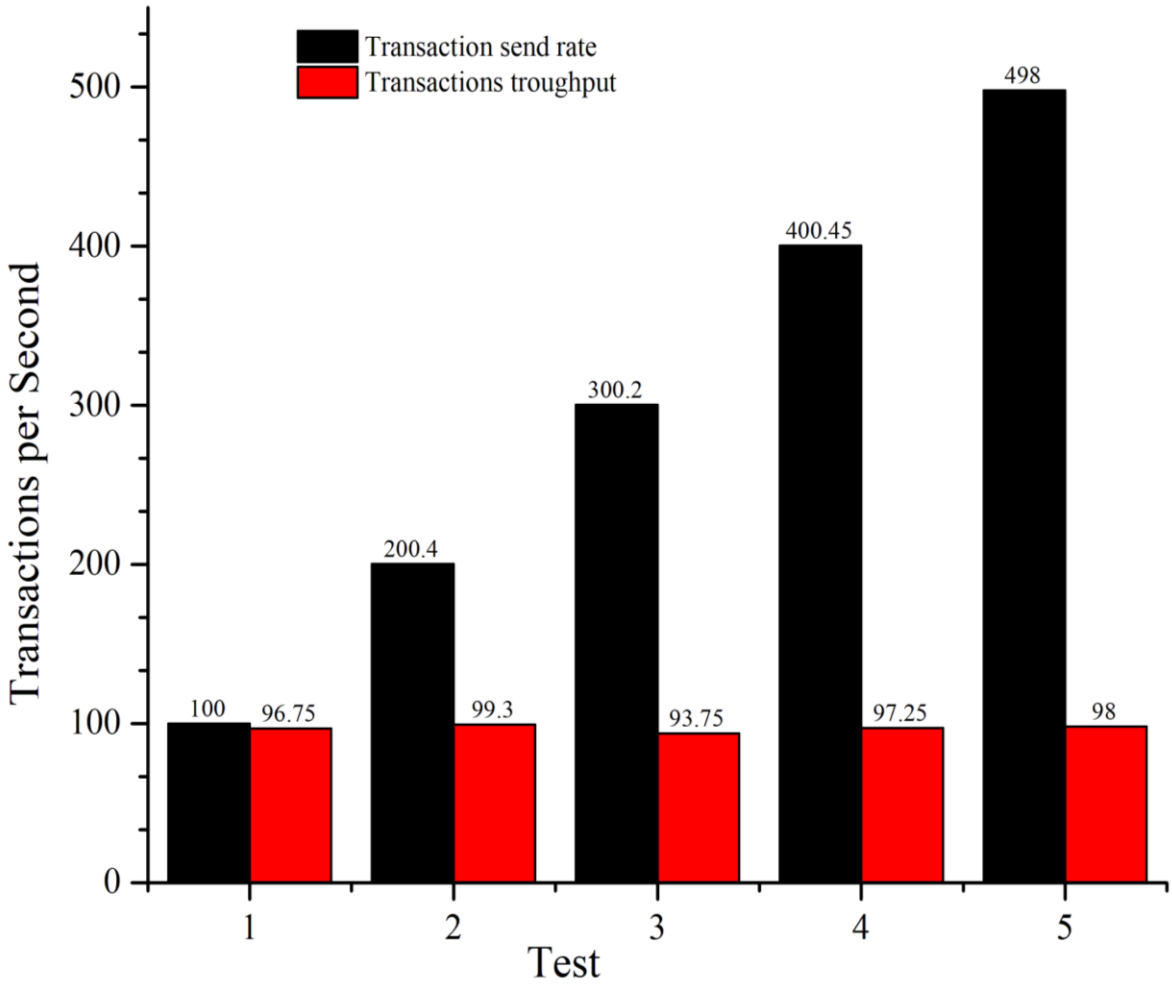

Figure 38: Transaction send rates and average throughputs per test

4.6 General discussion

This study aimed to develop a secure and interoperable blockchain-based information sharing system for healthcare providers in developing countries. To successfully achieve this goal; the following specific objectives were achieved: a) a study of the capabilities of currently available blockchain-based applications for healthcare information systems; b) analysis of the requirements of applicable blockchain-based applications that are most suitable for the environment of developing countries; c) development of a blockchain-based system(s) for healthcare providers and d) evaluation of the developed system(s). This chapter presented the results of each of the specific objectives through which Section 4.2 presented the results of the first objective, Section 4.3 presented the results of the second objective; and Sections 4.4 and 4.5 presented the results of the third and fourth objectives. Therefore, this section discusses the results presented in previous sections of this chapter.

The results of the first objective that evaluates the performance of the three most common blockchain-based health care systems (MedicalChain, Patientory and MediLedger) showed that the hyperledger based MedicalChain system exceeds the ethereum and parity platform systems (MediLedger and Patientory) in the execution of higher transactions per unit second, using RAM computing more transactions for 1 Mb of memory and computing higher transactions per 1 CPU cycle. Likewise, Dinh *et al.* (2017) reveal that hyperledger fabric applications exceed parity and ethereum in spite of using different evaluation metrics such as fault tolerance.

However, Pongnumkul *et al*. (2017) show that hyperledger fabrics achieve better throughput and latency in comparison to the ethereum framework. Similarly, other studies report the overall effectiveness of smart contracts on hyperledger fabrics that exceed smart contracts of other platforms (ethereum and parity) (Baliga *et al*., 2018; Nasir *et al*., 2018; Thakkar *et al.*, 2018). In addition, some studies propose that for confidentiality, safety purposes, and privacy hyperledger blockchains are safer than ethereum (Androulaki *et al.*, 2018; English *et al.*, 2018; Reyna *et al.*, 2018). As a result, it has been discovered that consortium-based blockchain platforms generally offer better performance than private and public blockchains.

The second objective examined the problems of electronic health systems in Tanzania, then proposed solutions to the discovered problems based on blockchain. The findings showed that there are difficulties in handling patients' private data, securely sharing medical information from one healthcare facility to another, addressing data integrity, and bandwidth-related issues. Blockchain technology provides solutions to these problems through self-sovereign identity and secure sharing of medical information using hyperledger fabric platforms and systems such as hyperledger fabric and interplanetary file system (Kombe *et al.*, 2019).

Therefore, this study developed a self-sovereign identity system that can be integrated with existing electronic health infrastructure to address privacy issues as recommended by the results of the second objective. Further, a decentralized and interoperable healthcare information sharing system with blockchain advanced security features was designed and developed. The proposed system has been implemented on a permissioned hyperledger fabric blockchain framework to allow secure sharing of information between EHR systems.

The third objective presented the designs and the development of the proposed systems through which two systems were designed and developed. The first system designed to address privacy issues, while the second system was developed to address data integrity issues and secure sharing of medical information from one healthcare facility to another. The development of a

self-sovereign identity system for the existing infrastructure (as described in Section 4.4) carried out in a virtual environment due to the sensitivity of health systems.

The development process used hyperledger indy, which is the self-sovereign identity development framework with all the cryptographic and other tools necessary for development. The system test was performed in a simulated environment with a statistical use model. The simulation included a government that acts as the steward in the definition of health insurance (NHIF), and two hospitals (Mt Meru and Arusha Lutheran Medical Centre (ALMC)). This study shows that it is possible to integrate a self-sovereign identity into the existing health infrastructure that does not provide this function. The integration of self-sovereign identity into existing systems has the following advantages: reduced development costs and the addition of privacy protection tools to existing infrastructures.

Ensuring the privacy of users' private data in an electronic system is a challenge. Different techniques have been used to address the problem, such as centralized and federated identity mechanisms that have shown great weakness in leaving users' private information such as email and passwords in the hands of hackers (Gunasinghe *et al.*, 2019). In addition, the private information provided by users of electronic systems has been sold to the black market, in particular, the internet, where, according to various studies, the healthcare sector is most affected by the problem (Czeschik, 2018; JA, 2015; Kan, 2016; Kaplan, 2016).

Self-sovereign identity addresses these issues by turning system users into owners of their private data. In healthcare systems, hiding information that can identify users from the owners of the system, such as hospitals, helps to use the remaining information for research, creating innovations; that can lead to the invention of new types of drugs. In addition, self-sovereign identity systems using blockchain technology eliminate the honeypot because of its ability to store only a few large amounts of data that normally attract hackers (Coelho *et al.*, 2018; Gordon & Catalini, 2018; Liang *et al.*, 2018; McGhin *et al.*, 2019; Onik *et al.*, 2019; Schanzenbach *et al.*, 2018).

In contrast, a decentralized and interoperable health information sharing system (as described in Section 4.5) that addresses data integrity issues and the secure sharing of medical information from one healthcare institution to another has been implemented on a permissioned hyperledger fabric blockchain framework. The system was developed to enable the secure sharing of information between two EHR systems (Care2x and OpenEMR) while preserving data integrity and confidentiality of patients' private data. The smart contract for this system

developed in JavaScript. The proposed system was tested for validation using hyperledger caliper version 0.20.8, a performance framework for testing blockchain-based systems.

The performance metrics tested were the success rate of the transactions, the latency of the transactions in seconds (s) and the performance of the transactions measured in transactions per unit of second (tps). The system received results of a 100% transaction success rate, an average minimum latency of 0.147 seconds, the overall average latency of 1.757 and 97.01 tps of average transaction throughput which indicate that the proposed system will experience good performance. The benefits of the proposed system over existing centralized systems include transparency, data integrity, protection against single-point-of-failure vulnerabilities, and prevention of internal threats such as untrusted system administrators.

Therefore, the research questions used in this study can be summarized in the findings as follows:

(i) What are the capabilities of the currently available blockchain-based applications for healthcare information systems?

According to the study, currently available blockchain-based applications for healthcare do the following; manage medical data, applied in the pharmaceutical supply chain, electronic health records, doctor prescription (Table 4). Unfortunately, the study found that there wasn't an application for integrating existing EHR systems which was also the gap filled by this study. Also, the performance of the three most common blockchain-based health care systems (MedicalChain, Patientory and MediLedger) evaluated in which the results showed that the hyperledger based MedicalChain system exceeds the ethereum and parity platform systems (MediLedger and Patientory) in the execution of higher transactions rate, using RAM computing more transactions for 1 Mb of memory and computing more transactions per 1 CPU cycle.

(ii) What are the blockchain-based requirements applicable for healthcare information system in developing countries environment?

To find the answer to this question, a qualitative research study was conducted to different healthcare facilities in Tanzania to examine the problems facing electronic healthcare systems then blockchain-based solutions were proposed to the discovered problems. The problems discovered were difficulties in handling patients' private data, securely sharing medical information from one healthcare facility to another, addressing data integrity, and bandwidth-related issues. Blockchain based solutions proposed for the discovered problems were self-

sovereign identity and secure sharing of medical information using hyperledger fabric platforms and systems such as hyperledger fabric and interplanetary file system.

(iii) What are the most effective designs, coding and verification methods of a blockchain based system appropriate for healthcare providers?

The proposed systems were developed in hyperledger fabric and hyperledger indy frameworks. Unified modelling language used to design the artefacts proposed for the systems. Programming languages such as Python, JavaScript, Java, JSON, and go used to develop different methods and smart contracts. Design science research methodology utilized to govern, manage and organize the development, validation, and verification process.

(iv) Did the proposed system developed in a right way?

The proposed system was tested through the hyperledger caliper. The results showed a 100% per cent success of the creation of credential definition which stored in blockchain ledger. For hyperledger caliper tests, the system received results of a 100% transaction success rate, an average minimum latency of 0.147 seconds, overall average latency of 1.757 and 97.01 tps of average transaction throughput which indicate that the proposed system will experience good performance.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

The purpose of this research study was to design an interoperable and secure information sharing system for healthcare systems in developing countries based on blockchain technology. The proposed system helps to solve the problems of interoperability, the privacy of stored patient information and the data integrity in existing healthcare systems. To achieve this objective the following tasks conducted: a) a study of the capabilities of currently available blockchain-based applications for healthcare information systems; b) analysis of the requirements of applicable blockchain-based applications that are most suitable for the environment of developing countries; c) development of a blockchain-based system(s) for healthcare providers and d) validation of the developed system(s).

The findings of this research lead to the development of two blockchain based systems: a) self-sovereign identity system for the existing healthcare information systems to address privacy issues and b) a decentralized and interoperable health information sharing system that addresses data integrity issues and the secure sharing of medical information from one healthcare institution to another. The benefits of these systems are; the addition of privacy protection tools to existing infrastructures, reduction of development cost, transparency, data integrity, protection against single-point-of-failure vulnerabilities, and prevention of internal threats such as untrusted system administrators.

The proposed systems will make the existing and future healthcare information systems trustable to healthcare service providers and the end-users of the healthcare systems. This is due to their ability of sharing sensitive information to different stakeholders without revealing the patients' identity information. Therefore, researchers' will be able to use medical records freely in their studies without a fear of violating privacy. On top of that, number of deaths which occur to referred patients due to lack of medical information from previous medical facilities and lead to readmission will decrease because proper information will be available in real time. On the other hand, accuracy and immutable audit trial in medical bills will increase as well as decrease of medical bills due to reduction of number of readmissions. In addition to that, the study will help the stakeholders in the healthcare sector to properly manage the healthcare systems. Furthermore, this study will contribute to knowledge whereby other researchers will benefit its findings.

5.2 Recommendations

Education and awareness concerning emerging technologies should be provided to the systems' administrators and other systems users in order for them to apply the gained knowledge and techniques to increase productivity and improve security. We also recommend to universities and other academic institutions to add blockchain technology to academic curriculums as will increase knowledge to graduates who among them are becoming experts in taking care of healthcare information systems and hence reduce researchers' time on explaining and educate them about the technology.

During the research it was observed that regulators such as Tanzania Communications Regulatory Authority (TCRA) and Tanzania Revenue Authority (TRA) and other regulators in developing countries are not proactive enough on setting regulation for emerging technologies specifically blockchain technology. We recommend to have such mechanism of studying and setting the regulation for the emerging technologies specifically blockchain technology which shows great potential for improving different domains.

This study suggests the following areas be taken into consideration for further studies:

(i) The standardization of interoperability of blockchain systems in healthcare domain
(ii) Further developments in extending the interoperability of public services through decentralized blockchain architecture which is more secure than what is existing today
(iii) More studies in self-sovereign identity to facilitate privacy and security of private data in a digital world

REFERENCES

Agarwal, A. (2019). *Elastico as an ordering service in Hyperledger Fabric* [Indian Institute of Technology Kanpur]. https://security.cse.iitk.ac.in/sites/default/files/17111010.pdf

Ahlan, A. R., & Isma, B. (2014). User Acceptance of Health Information Technology (HIT) in Developing Countries : A Conceptual Model. *Procedia Technology*, *16*, 1287–1296. https://doi.org/10.1016/j.protcy.2014.10.145

Al Omar, A., Rahman, M. S., Basu, A., & Kiyomoto, S. (2017). MediBchain: A blockchain based privacy preserving platform for healthcare data. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10658 LNCS*. https://doi.org/10.1007/978-3-319-72395-2_49

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., & Manevich, Y. (2018). Hyperledger fabric: A Distributed Operating System for Permissioned Blockchains. *Proceedings of the 13th EuroSys Conference*, 30.

Antonopoulos, A. M. (2015). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (M. Loukides & A. MacDonald (eds.); (1st ed.). O'Reilly Media.

Auffray, C., Balling, R., Barroso, I., Bencze, L., Benson, M., Bergeron, J., Bernal-Delgado, E., Blomberg, N., Bock, C., Conesa, A., Del Signore, S., Delogne, C., Devilee, P., Di Meglio, A., Eijkemans, M., Flicek, P., Graf, N., Grimm, V., Guchelaar, H. J., … Zanetti, G. (2016). Making sense of big data in health research: Towards an EU action plan. *Genome Medicine*, *8*(1), 71. https://doi.org/10.1186/s13073-016-0323-y

Baliga, A. (2017). Understanding Blockchain Consensus Models. In *Persistent Systems* (Issue April). https://www.persistent.com/wp-content/uploads/2017/04/WP-Understanding-Blockchain-Consensus-Models.pdf

Baliga, A., Subhod, I., Kamat, P., & Chatterjee, S. (2018). *Performance Evaluation of the Quorum Blockchain Platform*. http://arxiv.org/abs/1809.03421

Bamberger, M. (2000). Integrating Quntitative and Qualitative Research in Development Projects. In *World Bank*. http://www.wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2003/01/11/000094946_0212310400155/Rendered/PDF/multi0page.pdf

Benhamouda, F., Halevi, S., & Halevi, T. (2019). Supporting private data on Hyperledger

Fabric with secure multiparty computation. *IBM Journal of Research and Development*, *63*(2/3), 3:1-3:8. https://doi.org/10.1147/JRD.2019.2913621

Berg, B. L. (2008). *Qualitative Research Methods for the Social Sciences* (4th ed.). Pearson Education.

Booth, A., Hannes, K., Harden, A., Noyes, J., & Harris, J. (2014). COREQ (Consolidated Criteria for Reporting Qualitative Studies). In *Guidelines for reporting health research: a user's manual* (1st ed., pp. 1–320). Wiley-Blackwell Inc.; England.

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, *9*(2), 27–40.

Brodersen, C., Kalis, B., Leong, C., Mitchell, E., Pupo, E., & Truscott, A. (2016a). Blockchain : Securing a New Health Interoperability Experience. *NIST Workshop on Blockchain & Healthcare, August*, 1–11. https://doi.org/10.1001/jama.2012.362.4

Brodersen, C., Kalis, B., Leong, C., Mitchell, E., Pupo, E., & Truscott, A. (2016b). *Blockchain : Securing a New Health Interoperability Experience* (Issue August). https://doi.org/10.1001/jama.2012.362.4

Brogan, J., Baskaran, I., & Ramachandran, N. (2018). Authenticating Health Activity Data Using Distributed Ledger Technologies. *Computational and Structural Biotechnology Journal*, *16*, 257–266. https://doi.org/10.1016/j.csbj.2018.06.004

Bryman, A. (2012). *Social Research Methods* (4th ed.). Oxford University Press Inc.

Bryman, A. (2016). *Social Research Methods* (5th ed.). Oxford University Press Inc.

Cardoso, L., Marins, F., Portela, F., Santos, M., Abelha, A., & Machado, J. (2014). The next generation of interoperability agents in healthcare. *International Journal of Environmental Research and Public Health*, *11*(5), 5349–5371. https://doi.org/10.3390/ijerph110505349

Chen, Yi, Ding, S., Xu, Z., Zheng, H., & Yang, S. (2018). Blockchain-Based Medical Records Secure Storage and Medical Service Framework. *Journal of Medical Systems*, *43*(1). https://doi.org/10.1007/s10916-018-1121-4

Chen, Yongle, Li, H., Li, K., & Zhang, J. (2017). An improved P2P file system scheme based on IPFS and Blockchain. *2017 IEEE International Conference on Big Data (Big Data)*, 2652–2657.

Coelho, P., Zúquete, A., & Gomes, H. (2018). Federation of Attribute Providers for User Self-Sovereign Identity. *Journal of Information Systems Engineering & Management*, *3*(4), 2–7. https://doi.org/10.20897/jisem/3943

Creswell, J. W. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health Promotion Practice*, *16*(4), 473–475.

CSSC. (2017). *Experiences of FBOs in provision of health services under PPP framework*. CHRISTIAN SOCIAL SERVICES COMMISSION DEVELOPMENT (CSSC). http://www.tzdpg.or.tz/fileadmin/documents/dpg_internal/dpg_working_groups_clusters/cluster_2/health/DPGH_Meeting_Documents_2017/CSSC_Development_Partners_Presentation_Dec_2017.pdf

Czeschik, C. (2018). Black Market Value of Patient Data. In C. Linnhoff-Popien, R. Schneider, & M. Zaddach (Eds.), *Digital Marketplaces Unleashed* (pp. 883–893). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-49275-8_78

Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*, *39*, 283–297. https://doi.org/10.1016/j.scs.2018.02.014

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *JSTOR*, *13*(3), 319–340.

Dinh, T. T. A., Wang, J., Chen, G., Liu, R., Ooi, B. C., & Tan, K. L. (2017). Blockbench: A framework for analyzing private blockchains. *Proceedings of the 2017 ACM International Conference on Management of Data*, 1085–1100.

Domingo, S. A. I., & Enríquez, M. (2018). Digital Identity: the current state of affairs. In *BBVA Research*.

Dresch, A., Lacerda, D. P., & Antunes, J. A. V. (2015). Design Science Research. In *Design Science Research: A Method for Science and Technology Advancement* (pp. 67–102). Springer International Publishing. https://doi.org/10.1007/978-3-319-07374-3_4

Dunphy, P., & Petitcolas, F. A. P. (2018). A first look at identity management schemes on the blockchain. *IEEE Security & Privacy*, *16*(4), 20–29.

Ekblaw, A., Azaria, A., Halamka, J. D., Lippman, A., & Vieira, T. (2016). A Case Study for Blockchain in Healthcare: " MedRec " prototype for electronic health records and medical

research data. *2016 2nd International Conference on Open and Big Data*. https://www.healthit.gov/ sites/default/files/5-56-onc _blockchainchallenge_mitwhitepaper.pdf

English, E., Kim, A. D., & Nonaka, M. (2018). *Advancing Blockchain Cybersecurity : Technical and Policy Considerations for the Financial Services Industry* (Digital Chamber of Commerce).

Eyal, I., Gencer, A. E., Sirer, E. G., & Van Renesse, R. (2016). Bitcoin-NG: A Scalable Blockchain Protocol. *NSDI*, 45–59.

Fielding, M., Odero, B., & Ochieng, C. (2016). *From paper to data : taking medical health records into the future*.

Gale, N. K., Heath, G., Cameron, E., Rashid, S., & Redwood, S. (2013). Using the framework method for the analysis of qualitative data in multi-disciplinary health research. *BMC Medical Research Methodology*, *13*(1), 117. https://doi.org/10.1186/ 1471-2288-13-117

Garets, D., & Davis, M. (2005). Electronic Patient Records. *Healthcare Informatics Online*, *4*.

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report*, *8*(4), 597–607. https://doi.org/10.3367/UFNr.0180.201012c.1305

Goldwater, J. C. (2016). The Use of a Blockchain to Foster the Development of Patient-Reported Outcome Measures. *NIST Workshop on Blockchain & Healthcare*.

Gordon, W. J., & Catalini, C. (2018). Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. *Computational and Structural Biotechnology Journal*, *16*, 224–230. https://doi.org/10.1016/j.csbj.2018.06.003

Gropper, A. (2016). *Powering the Physician-Patient Relationship with HIE of One Blockchain Health IT*.

Gunasinghe, H., Kundu, A., Bertino, E., Krawczyk, H., Chari, S., Singh, K., & Su, D. (2019). PrivIdEx: Privacy Preserving and Secure Exchange of Digital Identity Assets. *The World Wide Web Conference*, 594–604.

Gupta, M. (2017). *Blockchain For Dummies: IBM Limited Edition* (1st ed.). John Wiley & Sons, Inc.

Haq, A., & Shabbir, J. (2014). An improved estimator of finite population mean when using two auxiliary attributes. *Applied Mathematics and Computation*, *241*, 14–24.

https://doi.org/10.1016/j.amc.2014.04.069

Hawig, D., Zhou, C., Fuhrhop, S., Fialho, A. S., & Ramachandran, N. (2019). Designing a Distributed Ledger Technology System for Interoperable and General Data Protection Regulation--Compliant Health Data Exchange: A Use Case in Blood Glucose Data. *Journal of Medical Internet Research*, *21*(6), e13665.

Hevner, A., & Chatterjee, S. (2010). Design Science Research Frameworks. In *Design Research in Information Systems: Theory and Practice* (pp. 23–31). Springer US. https://doi.org/10.1007/978-1-4419-5653-8_3

Hevner, A. R. (2007). A three cycle view of design science research. *Scandinavian Journal of Information Systems*, *19*(2), 4.

HL7. (2017). *About Health Level Seven International*. http://www.hl7.org/about/index.cfm?ref=nav

Hsieh, Y. Y., Vergne, J. P., & Wang, S. (2017). *The Internal and External Governance of Blockchain-Based Organizations: Evidence from Cryptocurrencies*.

Ichikawa, D., Kashiyama, M., & Ueno, T. (2017). Tamper-Resistant Mobile Health Using Blockchain Technology. *JMIR MHealth and UHealth*, *5*(7), 1–10. https://doi.org/10.2196/mhealth.7938

JA, A. (2015). *Hackers Selling Healthcare Data in the Black Market*. Info Sec. https://resources.infosecinstitute.com/ hackers-selling-healthcare -data-in-the-black-market/

Kajirunga, A., & Kalegele, K. (2015). Analysis of Activities and Operations in the Current E-Health Landscape in Tanzania : Focus on Interoperability and Collaboration. *International Journal of Computer Science and Information Security*, *13*(6), 49–54.

Kamau, G., Boore, C., Maina, E., & Njenga, S. (2018). Blockchain Technology: Is this the Solution to EMR Interoperability and Security Issues in Developing Countries? *2018 IST-Africa Week Conference (IST-Africa)*.

Kan, M. (2016). *Hacker looks to sell 10M patient records on black market | Computerworld*. Computer World. https://www.computerworld.com/article/3088972 /hacker-looks-to-sell-10m-patient-records-on-black-market.html

Kaplan, B. (2016). How Should Health Data Be Used?: Privacy, Secondary Use, and Big Data

Sales. *Cambridge Quarterly of Healthcare Ethics*, *25*(2), 312–329. https://doi.org/10.1017/S0963180115000614

Kombe, C., Ally, M., & Sam, A. (2018). A review on healthcare information systems and consensus protocols in blockchain technology. *International Journal of Advanced Technology and Engineering Exploration*, *5*(49), 473–483. https://doi.org/10.19101/IJATEE.2018.547023

Kombe, C., Sam, A., Ally, M., & Finne, A. (2019). Blockchain Technology in Sub-Saharan Africa: Where does it fit in Healthcare Systems: A case of Tanzania. *Journal of Health Informatics in Developing Countries*, *13*(2).

Krawiec, R., Barr, D., Killmeyer, J., Filipova, M., Quarre, F., Nesbitt, A., Fedosova, K., Tsai, L., & Israel, A. (2016). Blockchain : Opportunities for Health Care. In *NIST Workshop on Blockchain & Healthcare* (Issue August).

Laudon, K. C., & Laudon, J. P. (2016). *Management information system*. Pearson Education India.

Laurence, T. (2017). *Blockchain for dummies* (1st ed.). John Wiley & Sons, Inc.

Lemieux, V. L. (2016). Trusting records: is Blockchain technology the answer? *Records Management Journal*, *26*(2), 110–139. https://doi.org/10.1108/RMJ-12-2015-0042

Liang, X., Shetty, S., Zhao, J., Bowden, D., Li, D., & Liu, J. (2018). Towards decentralized accountability and self-sovereignty in healthcare systems. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 10631 LNCS*. https://doi.org/10.1007/978-3-319-89500-0_34

Linn, L. A., & Koo, M. B. (2014). *Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research*.

Linn, L. A., & Koo, M. B. (2016). Blockchain for health data and its potential use in health it and health care related research. *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*.

Magyar, G. (2018). Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management. *IEEE 30th Jubilee Neumann Colloquium, NC 2017*, *2018-January*. https://doi.org/10.1109/NC.2017.8263269

Mason, M. (2010). Sample size and saturation in PhD studies using qualitative interviews. *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, *11*(3).

McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, *135*, 62–75. https://doi.org/10.1016/j.jnca.2019.02.027

Mertz, L. (2018). (Block) chain reaction: A blockchain revolution sweeps into health care, offering the possibility for a much-needed data solution. *IEEE Pulse*, *9*(3), 4–7.

Milutinovic, M., He, W., Wu, H., & Kanwal, M. (2016). Proof of Luck: An efficient Blockchain consensus protocol. *Proceedings of the 1st Workshop on System Software for Trusted Execution*, 2.

Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., & Qijun, C. (2017). A Review on Consensus Algorithm of Blockchain. *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2567–2572. http://www.smc2017.org/SMC2017_Papers/media/files/0525.pdf

Miranda, M., Machado, J., Abelha, A., & Neves, J. (2013). Healthcare Interoperability through a JADE Based Multi-Agent Platform. In G. Fortino, C. Badica, M. Malgeri, & R. Unland (Eds.), *Intelligent Distributed Computing VI: Proceedings of the 6th International Symposium on Intelligent Distributed Computing - IDC 2012, Calabria, Italy, September 2012*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-32524-3_11

Mohanta, B. K., Panda, S. S., & Jena, D. (2018). An overview of smart contract and use cases in blockchain technology. *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 1–4.

MoHSW. (2013). Tanzania National eHealth Strategy 2012 - 2018. In *National eHealth Strategy* (Issue May 2013).

MoHSW. (2015). Health Sector Strategic Plan 2015-2020: Reaching all Households with Quality Health Care. In *United Republic of Tanzania Ministry of Health and Social Welfare* (Vol. 2020, Issue 7). https://doi.org/10.1016/j.msea.2006.03.069

Mtebe, J. S., & Nakaka, R. (2018). Assessing Electronic Medical Record System Implementation at Kilimanjaro Christian Medical Center, Tanzania. *Journal of Health Informatics in Developing Countries*, *12*(2).

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A Survey on Essential

Components of a Self-Sovereign Identity. *Computer Science Review*, *30*, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002

Mutale, W., Chintu, N., Amoroso, C., Awoonor-williams, K., Phillips, J., Baynes, C., Michel, C., Taylor, A., & Sherr, K. (2013). *Improving health information systems for decision making across five sub-Saharan African countries : Implementation strategies from the African Health Initiative*. *13*(Suppl 2), 1–12.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. In *Consulted*. https://doi.org/10.1007/s10838-008-9062-0

Nasir, Q., Qasse, I. A., Abu Talib, M., & Nassif, A. B. (2018). Performance Analysis of Hyperledger Fabric Platforms. *Security and Communication Networks*, *2018*.

Ndume, V., Nkansah-Gyekye, Y., & KO, J. (2013). Improving Data Collection and Integration of Electronic Healthcare Records in Tanzania. *2013 13th International Conference on Control, Automation and Systems*, *13*, 247–250.

Nehemiah, L. (2014). Towards EHR Interoperability in Tanzania Hospitals: Issues, Challenges and Opportunities. *International Journal of Computer Science, Engineering and Applications (IJCSEA)*, *4*(4), 29–36.

Nelson, R., & Staggers, N. (2016). *Health Informatics-E-Book: An Interprofessional Approach*. Elsevier Health Sciences.

Nguyen, L., Bellucci, E., & Nguyen, L. T. (2014). Electronic health records implementation : An evaluation of information system impact and contingency factors. *International Journal of Medical Informatics*, *83*(11), 779–796. https://doi.org/10.1016/j.ijmedinf.2014.06.011

O'Leary, Z. (2004). *The Essential Guide to Doing Research* (1st ed.). SAGE Publications Ltd.

O'reilly, M., & Parker, N. (2013). 'Unsatisfactory Saturation': a critical exploration of the notion of saturated sample sizes in qualitative research. *Qualitative Research*, *13*(2), 190–197.

Onik, M. M. H., Aich, S., Yang, J., Kim, C. S., & Kim, H. C. (2019). Blockchain in Healthcare: Challenges and Solutions. *Big Data Analytics for Intelligent Healthcare Management*, 197–226. https://doi.org/10.1016/B978-0-12-818146-1.00008-8

Ozair, F. F., Jamshed, N., Sharma, A., & Aggarwal, P. (2015). Ethical issues in electronic

health records: A general overview. *Perspectives in Clinical Research*, *6*(2), 73–76. https://doi.org/10.4103/2229-3485.153997

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*, *42*(5), 533–544.

Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In *Banking Beyond Banks and Money* (pp. 239–278). Springer.

Pongnumkul, S., Siripanpornchana, C., & Thajchayapong, S. (2017). Performance analysis of private blockchain platforms in varying workloads. *2017 26th International Conference on Computer Communications and Networks, 2017*. https://doi.org/ 10.1109/ICCCN.2017.8038517

Poore, J. H. (1999). Application of Statistical Science to Testing and Evaluating Software Intensive Systems. In *Statistics, Testing, and Defense Acquisition: Background Papers* (pp. 124–170). National Academies Press. https://doi.org/10.17226/9655

Rahman, S. M. M. (2014). Towards integrity protection of software for e-health data. *Multimedia and Expo Workshops (ICMEW), 2014 IEEE International Conference On*, 1–5.

Reyna, A., Mart\'\in, C., Chen, J., Soler, E., & D\'\iaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*.

Ritchie, J., Lewis, J., Nicholls, C. M., & Ormston, R. (2013). *Qualitative research practice: A guide for social science students and researchers*. sage.

Rubin, A. (2014). *Research Methods for Social Work* (8th ed.). Brooks/Cole Empowerment Series. http://www.amazon.com/dp/0 495811718

Samuel, R. E. (2016). A Layered Architectural Approach To Understanding Distributed Cryptographic Ledgers. *Issues in Information Systems*, *17*(IV), 222–226.

Schanzenbach, M., Bramm, G., & Schutte, J. (2018). ReclaimID: Secure, Self-Sovereign Identities Using Name Systems and Attribute-Based Encryption. *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and*

Engineering, *Trustcom/BigDataSE 2018*, 946–957. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00134

Shu, C. (2019). *Dual replication: a novel byzantine fault tolerance consensus algorithm in hyperledger fabric*. Hong Kong Polytechnic University.

Sikorski, J. J., Haughton, J., & Kraft, M. (2017). Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Applied Energy*, *195*, 234–246.

Soceanu, A., Vasylenko, M., Egner, A., & Muntean, T. (2015). Managing the privacy and security of ehealth data. *Control Systems and Computer Science (CSCS), 2015 20th International Conference On*, 439–446.

Sousa, J., Bessani, A., & Vukolić, M. (2017). A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform. *ArXiv Preprint ArXiv:1709.06921*.

Stake, R. E. (2010). Qualitative Research: Studying How Things Works. In *Journal of Chemical Information and Modeling* (1st ed., Vol. 53). The Guilford Press. https://doi.org/10.1017/CBO9781107415324.004

Swan, M. (2015). *Blockchain* (1st ed.). O'Reilly Media. http://safaribooksonline.com

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution* (1st ed.). Penguin Random House LLC.

Thakkar, P., Nathan, S., & Vishwanathan, B. (2018). *Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform*. http://arxiv.org/abs/1805.11390

Thomas, L., Zhou, Y., Long, C., Wu, J., & Jenkins, N. (2019). A general form of smart contract for decentralized energy systems management. *Nature Energy*, *4*(2), 140.

Thummavet, P. (2019). *Demystifying Hyperledger Fabric (1/3): Fabric Architecture*. Medium. https://medium.com/coinmonks/demystifying-hyperledger-fabric-1-3-fabric-architecture-a2fdb587f6cb

Vaishnavi, V. K., & Kuechler, W. (2015). *Design science research methods and patterns: innovating information and communication technology*. Crc Press.

van der Merwe, A., Gerber, A., & Smuts, H. (2017). Mapping a Design Science Research Cycle to the Postgraduate Research Report. *ICT Education*.

Venable, J. R., Pries-heje, J., & Baskerville, R. (2017). Choosing a Design Science Research Methodology. *Australasian Conference on Information Systems*, 1–11. https://www.

acis2017.org/wp-content/uploads/2017/11/ACIS2017_paper_2 55_FULL .pdf

Wang, H., & Song, Y. (2018). Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain. *Journal of Medical Systems*, *42*(8). https://doi.org/ 10.1007/s10916-018-0994-6

White, F. (2015). Primary Health Care and Public Health : Foundations of Universal Health Systems. *Medical Principles and Practice*, *24*, 103–116. https://doi.org/10.1159/ 000370197

William, C. (2017). 22 Privacy and Security: Privacy of Personal eHealth Data in Low-and Middle-Income Countries. *Global Health Informatics: Principles of EHealth and MHealth to Improve Quality of Care*, 269.

World Economic Forum. (2018). Identity in a Digital World A new chapter in the social contract Insight Report. In *World Economic Forum*, *USA* (Issue September). www.weforum.org

World Health Organization. (2007). *Everybody business : strengthening health systems to improve health outcomes : WHO's framework for action*. https://doi.org/978 92 4 159607 7

World Health Organization. (2017). *World health statistics 2017: monitoring health for the SDGs, Sustainable Development Goals*.

Xiong, W., & Xiong, L. (2019). Smart contract based data trading mode using blockchain and machine learning. *IEEE Access*, *7*, 102331–102344.

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., & Rimba, P. (2017). A Taxonomy of Blockchain-Based Systems for Architecture Design. *Proceedings - 2017 IEEE International Conference on Software Architecture, ICSA 2017*, 243–252. https://doi.org/10.1109/ICSA.2017.33

Yamashita, K., Nomura, Y., Zhou, E., Pi, B., & Jun, S. (2019). Potential Risks of Hyperledger Fabric Smart Contracts. *2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, 1–10. https://doi.org/10.1109/IWBOSE. 2019.8666486

Yin, R. K. (2015). *Qualitative Research from Start to Finish* (2nd ed.). The Guilford Press.

Zhang, A., & Lin, X. (2018). Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. *Journal of Medical Systems*, *42*(8).

https://doi.org/10.1007/s10916-018-0995-5

Zheng, P., Zheng, Z., Luo, X., Chen, X., & Liu, X. (2018). A detailed and real-time performance monitoring framework for blockchain systems. *Proceedings of the 40th International Conference on Software Engineering Software Engineering in Practice - ICSE-SEIP '18*, 134–143. https://doi.org/10.1145/3183519.3183546

Zheng, Z., Xie, S., Dai, H. N., & Wang, H. (2016). Blockchain challenges and opportunities: A survey. *Work Pap*.

APPENDICES

Appendix 1: Questionnaire to system users from healthcare providers

My name is KOMBE, CLEVERENCE from the Nelson Mandela African Institution of Science and Technology (NM-AIST). I am doing research on a secure and interoperable blockchain-based information sharing system for healthcare providers in developing countries. Dr. Anael E. Sam is supervising the research as principal supervisor and Dr. Mussa Ally a co-supervisor. We have chosen your institution as one of our case studies.

The purpose of this research study is to design an interoperable and secure information sharing system for healthcare systems in developing countries based on blockchain technology. The proposed system will help to solve the problems of interoperability, the privacy of stored patient information and the data integrity in existing healthcare systems. To achieve this objective; 1) the capabilities of the currently available blockchain-based applications for healthcare information systems will be investigated, 2) the requirements of applicable blockchain-based applications most appropriate for developing countries environment will be analysed, 3) the blockchain based system for healthcare providers will be developed and implemented and 4) the developed system will be validated.

The findings of this research will lead to the development of a blockchain based system for Electronic Health Records (EHRs) which will help in solving the problems of interoperability, the privacy of patient information and integrity of the patient's data. Also, the study will help the stakeholders in healthcare sector to properly manage the healthcare systems. Additionally, this study will contribute to knowledge whereby other researcher will benefits its findings.

We request your opinion to all issues related to the existing healthcare systems to your area. I assure you that everything you tell me will be confidential and your name or title will not be used in survey records, unless you authorize.

Name of Researcher: ……

Signature: ……

Date: …….

OPEN ENDED QUESTIONS

1. When was your electronic health record (EHR) was installed?
2. How many times your EHR has been updated/upgraded?
3. Is it an opensource/a proprietary/ in house-built software?
4. On which platform does your system operate?
5. What type of database does the system use?
6. How is the database configured? Example: Centralized or Distributed
7. Did the EHR system require the healthcare organization to purchase any additional proprietary software? If YES, could you provide the names of additional software?
8. Does the EHR use HL7 interfacing/messaging standards?
9. Does your EHR have the capability to upload digital files? If so what format?
10. Does the EHR offers total paperless operation? If not, does the EHR allow the capability to scan reports?
11. Are the doctors at your institution able to access the system from anywhere via Internet connection or does the system require the use of central login functionality? Could you please describe doctor's internal and external access procedures?
12. Does your EHR have capabilities of integrating with other software/programs? If yes list the software/programs integrated to your EHR
13. What are the security features of the your EHR system?
14. Are there access audits available from the system and who monitors these audit trails?
15. What functions are available to your EHR end users while accessing the system? Example: delete, update, inserting etc
16. Can updates be appended and/or changed and does this impact the doctor signing process?
17. Could anyone else outside your institution allowed access to the EHR? How is the access monitored and why?
18. Has the department allowed any staff to work remotely as a result of the EHR implementation? Which positions? Explain.
19. Are patients allowed to review their medical records electronically? If YES, what are the procedure they have to follow to make the review?

"THANK YOU FOR SPENDING YOUR TIME PARTICIPATING IN THIS RESEARCH''

Appendix 2: Introduction letter from the Nelson Mandela African Institution of Science and Technology

THE NELSON MANDELA
AFRICAN INSTITUTION OF SCIENCE AND TECHNOLOGY
(NM-AIST)
School of Computational and Communication Science and Engineering

Direct Line: +255 272970001
Fax: +255 272970016
E-mail: dean-cocse@nm-aist.ac.tz

Tengeru
P.O. Box 447
Arusha, TANZANIA
Website: www.nm- aist.ac.tz

OUR Ref.No. NM-AIST/P.174/T.16/10 **Date:** 22th Januray, 2018

To Whom It May Concern,

Dear Sir/Madam,

RE: INTRODUCTION OF MR. CLEVERENCE KOMBE

Kindly refer to the above heading.

I wish to introduce Mr. Cleverence Kombe with Registration No. NM-AIST/P.174 who is a PhD student at the Nelson Mandela African Institution of Science and Technology under School of Computational and Communication Science and Engineering. As part of the requirement for PhD degree, Mr. Cleverence is undertaking a research with title **"A Secure and Interoperable Blockchain – Based Information Sharing System for Healthcare Providers in Developing Countries".**

In order to accomplish his research objectives, he would like to collect some information from your organization. The information collected will be used for research purposes only and will provide a picture on the issue of Information Sharing System for Healthcare in Tanzania as it states in the research objectives.

It is my sincere hope you will assist him in accomplishing the study.

Looking forward for your cooperation.

Yours Sincerely,

Shubi Kaijage,*PhD*
Ag. Dean, School of CoCSE

Nelson Mandela African Institute of Science and Technology
(NM AIST - ARUSHA)
P. O. Box 447
Tel: +255 27 2555070

Appendix 3: Permission Letter from Arusha Regional Administrative Secretary office

UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE
REGIONAL ADMINISTRATION AND LOCAL GOVERNMENT

Telegrams: **"REGCOM"**
Telephone:**2545608/2544950/2544802**
Fax No. **2545239/254486**
E-Mail: ras@arusha.go.tz
E-Mail: ras.arusha@tamisemi.go.tz
Website: www.arusha.go.tz
In reply please quote:
Ref. No. FA.195/223/01'J'/388

REGIONAL COMMSSIONER'S OFFICE,
P.O. Box 3050,
ARUSHA.

12th February, 2018

Regional Medical Officer,
Mt. Meru Referral Hospital,
P. O. Box 3092,
ARUSHA.

RE: RESEARCH PERMIT

Reference is hereby made to the letter Ref.No. NM-AIST/P. 174/T.16/10 dated 22 January, 2018 from The Dean, School of CoCES, The Nelson Mandela African Institution of Science and Technology concerning the above underlined subject.

I hereby taking this opportunity to introduce to you **Mr. Cleverence Kombe** at the moment conducting a research titled ***"A Secure and Interoperable Blockchain – Based Information Sharing System for Healthcare Providers in Development Countries".***

He has been granted permission to conduct his research at Arusha District from **one week.** Due to this, you are requested to render any necessary Administrative Assistance to enable him to accomplish the intended objective of his research.

Your cooperation is highly expected.

(A.J. Mushashu)
For: **REGIONAL ADMINISTRATIVE SECRETARY**
ARUSHA

Copy to:
Mr. Cleverence Kombe,
Student of NM- AIST

Appendix 4: Python code: Getting Trust Anchor credentials for NHIF, Mt_Meru, ALMC and Government

```
"    print(\"=============================\")\n",
    "    print(\"=== Getting Trust Anchor credentials for NHIF, Mt_Meru, ALMC and Government  ==\")\n",
    "    print(\"-----------------------------\")\n",
    "\n",
    "    print(\"\\\"Government Steward\\\" -> Create wallet\")\n",
    "    steward = {\n",
    "        'name': \"Government Steward\",\n",
    "        'wallet_config': json.dumps({'id': 'sovrin_steward_wallet'}),\n",
    "        'wallet_credentials': json.dumps({'key': 'steward_wallet_key'}),\n",
    "        'pool': pool_['handle'],\n",
    "        'seed': '000000000000000000000000Steward1'\n",
    "    }\n",
    "\n",
    "    try:\n",
    "        await wallet.create_wallet(steward['wallet_config'], steward['wallet_credentials'])\n",
    "    except IndyError as ex:\n",
    "        if ex.error_code == ErrorCode.WalletAlreadyExistsError:\n",
    "            pass\n",
    "\n",
    "    steward['wallet'] = await wallet.open_wallet(steward['wallet_config'], steward['wallet_credentials'])\n",
    "\n",
    "    print(\"\\\"Government Steward\\\" -> Create and store in Wallet DID from seed\")\n",
    "    steward['did_info'] = json.dumps({'seed': steward['seed']})\n",
    "                steward['did'], steward['key'] = await did.create_and_store_my_did(steward['wallet'], steward['did_info'])\n",
    "\n",
```

Appendix 5: Python code: Getting Trust Anchor credentials - Government Onboarding

```
"    print(\"================================\")\n",
    "    print(\"== Getting Trust Anchor credentials - Government Onboarding  ==\")\n",
    "    print(\"--------------------------------\")\n",
    "\n",
    "    government = {\n",
    "        'name': 'Government',\n",
    "        'wallet_config': json.dumps({'id': 'government_wallet'}),\n",
    "        'wallet_credentials': json.dumps({'key': 'government_wallet_key'}),\n",
    "        'pool': pool_['handle'],\n",
    "        'role': 'TRUST_ANCHOR'\n",
    "    }\n",
    "    steward['did_for_government'], steward['key_for_government'], government['did_for_steward'], \\\n",
    "    government['key_for_steward'], _ = await onboarding(steward, government)\n",
    "\n",
    "    print(\"================================\")\n",
    "    print(\"== Getting Trust Anchor credentials - Government getting Verinym  ==\")\n",
    "    print(\"--------------------------------\")\n",
    "\n",
    "    government['did'] = await get_verinym(steward, steward['did_for_government'],
steward['key_for_government'],\n",
    "                                          government, government['did_for_steward'], government['key_for_steward'])\n",
    "\n",
```

Appendix 6: Python code Getting Trust Anchor credentials - NHIF Onboarding

```
"    print(\"================================\")\n",
    "    print(\"== Getting Trust Anchor credentials - NHIF Onboarding  ==\")\n",
    "    print(\"--------------------------------\")\n",
    "\n",
    "    nhif = {\n",
    "        'name': 'NHIF',\n",
    "        'wallet_config': json.dumps({'id': 'nhif_wallet'}),\n",
    "        'wallet_credentials': json.dumps({'key': 'nhif_wallet_key'}),\n",
    "        'pool': pool_['handle'],\n",
    "        'role': 'TRUST_ANCHOR'\n",
    "    }\n",
    "    steward['did_for_nhif'], steward['key_for_nhif'], nhif['did_for_steward'], nhif['key_for_steward'], _ = \\\n",
    "        await onboarding(steward, nhif)\n",
    "\n",
    "    print(\"================================\")\n",
    "    print(\"== Getting Trust Anchor credentials - NHIF getting Verinym  ==\")\n",
    "    print(\"--------------------------------\")\n",
    "\n",
    "    nhif['did'] = \\\n",
    "        await get_verinym(steward, steward['did_for_nhif'], steward['key_for_nhif'],\n",
    "                          nhif, nhif['did_for_steward'], nhif['key_for_steward'])\n",
    "\n",
```

Appendix 7: Python code: Getting Trust Anchor credentials - Mt_Meru Onboarding

```
"    print(\"=============================\")\n",
"    print(\"== Getting Trust Anchor credentials - Mt_Meru Onboarding  ==\")\n",
"    print(\"-----------------------------\")\n",
"\n",
"    mt_meru = {\n",
"        'name': 'Mt_Meru',\n",
"        'wallet_config': json.dumps({'id': 'mt_meru_wallet'}),\n",
"        'wallet_credentials': json.dumps({'key': 'mt_meru_wallet_key'}),\n",
"        'pool': pool_['handle'],\n",
"        'role': 'TRUST_ANCHOR'\n",
"    }\n",
"                    steward['did_for_mt_meru'],      steward['key_for_mt_meru'],      mt_meru['did_for_steward'],
mt_meru['key_for_steward'], _ = \\\n",
"        await onboarding(steward, mt_meru)\n",
"\n",
"    print(\"=============================\")\n",
"    print(\"== Getting Trust Anchor credentials - Mt_Meru getting Verinym  ==\")\n",
"    print(\"-----------------------------\")\n",
"\n",
"    mt_meru['did'] = await get_verinym(steward, steward['did_for_mt_meru'], steward['key_for_mt_meru'],\n",
"                                       mt_meru, mt_meru['did_for_steward'], mt_meru['key_for_steward'])\n",
"\n",
```

Appendix 8: Python code: Getting Trust Anchor credentials - ALMC Onboarding

```
"    print(\"=============================\")\n",
    "    print(\"== Getting Trust Anchor credentials - ALMC Onboarding  ==\")\n",
    "    print(\"------------------------------\")\n",
    "\n",
    "    almc = {\n",
    "        'name': 'ALMC',\n",
    "        'wallet_config': json.dumps({'id': 'almc_wallet'}),\n",
    "        'wallet_credentials': json.dumps({'key': 'almc_wallet_key'}),\n",
    "        'pool': pool_['handle'],\n",
    "        'role': 'TRUST_ANCHOR'\n",
    "    }\n",
    "     steward['did_for_almc'], steward['key_for_almc'], almc['did_for_steward'], almc['key_for_steward'], _ =
\\\n",
    "        await onboarding(steward, almc)\n",
    "\n",
    "    print(\"=============================\")\n",
    "    print(\"== Getting Trust Anchor credentials - ALMC getting Verinym  ==\")\n",
    "    print(\"------------------------------\")\n",
    "\n",
    "    almc['did'] = await get_verinym(steward, steward['did_for_almc'], steward['key_for_almc'],\n",
    "                                    almc, almc['did_for_steward'], almc['key_for_steward'])\n",
    "\n",
```

Appendix 9: Python code: Credential Schemas Setup

```
"    print(\"==============================\")\n",
"    print(\"=== Credential Schemas Setup ==\")\n",
"    print(\"------------------------------\")\n",
"\n",
"    print(\"\\\"Government\\\" -> Create \\\"Patient\\\" Schema\")\n",
"    patient = {\n",
"        'name': 'Patient',\n",
"        'version': '0.2',\n",
"        'attributes': ['first_name', 'last_name', 'salary', 'employee_status', 'experience']\n",
"    }\n",
"    (government['patient_schema_id'], government['patient_schema']) = \\\n",
"        await anoncreds.issuer_create_schema(government['did'], patient['name'], patient['version'],\n",
"                                             json.dumps(patient['attributes']))\n",
"    patient_schema_id = government['patient_schema_id']\n",
"\n",
"    print(\"\\\"Government\\\" -> Send \\\"Patient\\\" Schema to Ledger\")\n",
"                        await send_schema(government['pool'], government['wallet'], government['did'],
government['patient_schema'])\n",
"\n",
"    print(\"\\\"Government\\\" -> Create \\\"Insurance\\\" Schema\")\n",
"    insurance = {\n",
"        'name': 'Insurance',\n",
"        'version': '1.2',\n",
"        'attributes': ['first_name', 'last_name', 'degree', 'status', 'year', 'average', 'ssn']\n",
"    }\n",
"    (government['insurance_schema_id'], government['insurance_schema']) = \\\n",
"        await anoncreds.issuer_create_schema(government['did'], insurance['name'], insurance['version'],\n",
"                                             json.dumps(insurance['attributes']))\n",
"    insurance_schema_id = government['insurance_schema_id']\n",
"\n",
"    print(\"\\\"Government\\\" -> Send \\\"Insurance\\\" Schema to Ledger\")\n",
"                        await send_schema(government['pool'], government['wallet'], government['did'],
government['insurance_schema'])\n",
"\n",
"    time.sleep(1)  # sleep 1 second before getting schema\n",
"\n",
```

Appendix 10: Python code: NHIF Credential Definition Setup

```
"    print(\"==============================\")\n",
   "    print(\"=== NHIF Credential Definition Setup ==\")\n",
   "    print(\"------------------------------\")\n",
   "\n",
   "    print(\"\\\"NHIF\\\" -> Get \\\"Insurance\\\" Schema from Ledger\")\n",
   "    (nhif['insurance_schema_id'], nhif['insurance_schema']) = \\\n",
   "        await get_schema(nhif['pool'], nhif['did'], insurance_schema_id)\n",
   "\n",
   "    print(\"\\\"NHIF\\\" -> Create and store in Wallet \\\"NHIF Insurance\\\" Credential Definition\")\n",
   "    insurance_cred_def = {\n",
   "        'tag': 'TAG1',\n",
   "        'type': 'CL',\n",
   "        'config': {\"support_revocation\": False}\n",
   "    }\n",
   "    (nhif['insurance_cred_def_id'], nhif['insurance_cred_def']) = \\\n",
   "        await anoncreds.issuer_create_and_store_credential_def(nhif['wallet'], nhif['did'],\n",
   "                                                    nhif['insurance_schema'], insurance_cred_def['tag'],\n",
   "                                                    insurance_cred_def['type'],\n",
   "                                                    json.dumps(insurance_cred_def['config']))\n",
   "\n",
   "    print(\"\\\"NHIF\\\" -> Send  \\\"NHIF Insurance\\\" Credential Definition to Ledger\")\n",
   "    await send_cred_def(nhif['pool'], nhif['wallet'], nhif['did'], nhif['insurance_cred_def'])\n",
   "\n",
   "    print(\"==============================\")\n",
   "    print(\"=== Mt_Meru Credential Definition Setup ==\")\n",
   "    print(\"------------------------------\")\n",
   "\n",
   "    print(\"\\\"Mt_Meru\\\" -> Get from Ledger \\\"Patient\\\" Schema\")\n",
   "    (mt_meru['patient_schema_id'], mt_meru['patient_schema']) = \\\n",
   "        await get_schema(mt_meru['pool'], mt_meru['did'], patient_schema_id)\n",
   "\n",
   "    print(\"\\\"Mt_Meru\\\" -> Create and store in Wallet \\\"Mt_Meru Patient\\\" Credential Definition\")\n",
   "    patient_cred_def = {\n",
   "        'tag': 'TAG1',\n",
   "        'type': 'CL',\n",
   "        'config': {\"support_revocation\": False}\n",
   "    }\n",
```

```
"    (mt_meru['patient_cred_def_id'], mt_meru['patient_cred_def']) = \\\n",
"        await anoncreds.issuer_create_and_store_credential_def(mt_meru['wallet'], mt_meru['did'],\n",
"                                                mt_meru['patient_schema'],\n",
"                                                patient_cred_def['tag'],\n",
"                                                patient_cred_def['type'],\n",
"                                                json.dumps(patient_cred_def['config']))\n",
"\n",
"    print(\"\\\"Mt_Meru\\\" -> Send \\\"Mt_Meru Patient\\\" Credential Definition to Ledger\")\n",
"    await send_cred_def(mt_meru['pool'], mt_meru['wallet'], mt_meru['did'], mt_meru['patient_cred_def'])\n",
"\n",
```

Appendix 11: JavaScript smart contract to define transactions and context

```
// Fabric smart contract classes
const { Contract, Context } = require('fabric-contract-api');
/**
 * A custom context provides access to list of all success patients transactions
 */
class PatientContext extends Context {

   constructor() {
      super();
   }
/**
 * Define EHR interoperability smart contract by extending Fabric Contract class
 *
 */
}
class EhrInteroperabilityContract extends Contract {
   constructor() {
      super();
   }
class EhrInteroperabilityContract extends Contract {

            async save(ctx, facilityID, facilityName, patientID, patientAge,patientWeight,
            claim,prescription,visitDate, physicianID) {

      let ptransaction = EhrInteroperabiltity.createInstance(facilityID, facilityName, patientID,
               patientAge,patientWeight,claim,prescription,visitDate, physicianID);

       ptransaction.setSaved();

       await ctx.patientTransList.addTransaction(ptransaction);

       return ptransaction;

            }

 constructor() {
      super();
   }

      createContext() {
```

```
        return new PatientContext();
    }

    /**
     * Instantiate to perform any setup of the ledger that might be required.
     * @param {Context} ctx the transaction context
     */
    async instantiate(ctx) {
        console.log('Instantiate the contract');
    }

    /**
     * Save patients transactions
     *
     * @param {Context} ctx
     * @param {Integer} facilityID
     * @param {String} facilityName
     * @param {Integer} patientID
     * @param {Integer} patientAge
     * @param {Integer} patientWeight
     * @param {String} claim
     * @param {String} prescription
     * @param {String} visitDate
     * @param {Integer} physicianID
    */
    async save(ctx, facilityID, facilityName, patientID, patientAge,patientWeight,claim,prescription,visitDate, physicianID) {
        let ptransaction = EhrInteroperabiltity.createInstance(facilityID, facilityName, patientID, patientAge,patientWeight,claim,prescription,visitDate, physicianID);
        ptransaction.setSaved();
        await ctx.patientTransList.addTransaction(ptransaction);
        return ptransaction;
    }
}
```